Smart5Grid

Demonstration of **5G** solutions for
SMART energy **GRID**s of the future

Deliverable D2.2

Overall Architecture Design, Technical Specifications and Technology Enablers

Version 2.0 - Date 24/02/2022

5G PPP
The 5G Infrastructure Public Private Partnership

This project has received funding from the European Union's *Horizon 2020 research and innovation programme* under grant agreement n° 101016912

D2.2 – Overall Architecture Design, Technical Specifications and Technology Enablers

Document Information

Programme	Horizon 2020 Framework Programme – Information and Communication Technologies
Project acronym	Smart5Grid
Grant agreement number	101016912
Number of the Deliverable	D2.2
WP/Task related	WP2/ T2.2, T2.3
Type (distribution level)	PU Public
Date of delivery	24-02-2022
Status and Version	Version 2.0
Number of pages	156 pages
Document Responsible	Borja Otura / Paula Encinar – ATOS
Author(s)	Anastasios Lytos – SID Andrés Cárdenas - i2CAT Angelos Antonopoulos - NBC Athanasios Bachoumis – UBE Arif Ishaq – ATH August Betzler - i2CAT Borja Otura – ATOS Daniele Munaretto – ATH Dimitris Brodimas – IPTO Eugenia Vergi – INF Gianluca Rizzi – W3 Ioannis Chochliouros – OTE

Irina Ciornei – UCY
Juliana Teixeira – UW
Lenos Hadjidemetriou – UCY
Luigi Sechi – STAM
Luís Conceição – UW
Marco Centenaro - ATH
Markos Asprou – UCY
Nicola Cadenelli – NBC
Nicola di Pietro – ATH
Paula Encinar - ATOS
Sonia Castro – ATOS
Theocharis Saoulidis – SID
Theoni Dounia – INF
Yanos Angelopoulos – AXON

Reviewers

Anastasis Tzoumpas – UBE
Antonello Corsi – ENG
Gianluca Rizzi – W3
Ioannis Chochliouros – OTE
Nick Vrionis – INF
Nicola di Prieto – ATH
Sonia Castro – ATOS

Revision History

Version	Date	Author/Reviewer	Notes
0.1	13/03/2021	Sonia Castro	Initial table of content for feedback
0.2	22/03/2021	Borja Otura	Feedback to Initial ToC
0.3	22/03/2021	Antonello Corsi	Feedback to Initial ToC
0.4	26/03/2021	Sonia Castro	Restructured ToC based on additional comments
0.5	21/05/2021	Sonia Castro	Notations, abbreviations, and acronyms moved as suggested in D2.1
0.6	21/05/2021	Sonia Castro	ToC restructuration
0.7	23/06/2021	Borja Otura	Consolidation of bullet point contribution from partners
0.8	14/07/2021	Borja Otura	Consolidation of first draft contributions
0.9	28/07/2021	Borja Otura	Consolidation of final round of contributions
0.10	02/08/2021	Sonia Castro	Version for internal review
0.11	04/08/2021	Sonia Castro	Updated version for internal review
0.12	05/08/2021	Sonia Castro	Updated version for internal review 2
0.13	17/08/2021	Borja Otura	Updated version for internal review 3
0.14	23/08/2021	Borja Otura	Comments from Internal Review addressed
0.15	09/09/2021	Borja Otura	Version for External Review
0.16	21/09/2021	Borja Otura	Version for Quality review
0.17	22/09/2021	Daniele Porcu	Minor quality editing adjustments
0.18	22/09/2021	Daniele Porcu	Version ready for Project Board approval
1.0	29/09/2021	Borja Otura	Release approved by PB.
1.1	26/01/2022	All	Reaction to Review report, "Data Flows and Management" sessions added in each UC's dedicated NetApp
1.2	20/02/2022	Borja Otura, All	Version finalized, ready for review
2.0	24/02/2022	Borja Otura	Release approved by PB.

Executive summary

Smart5Grid´s objective is to revolutionize the energy vertical sector by adopting the latest advancements in 5G technologies to address four essential functions of smart grids: i) automatic power distribution grid fault detection, ii) remote inspection of automatically delimited working areas at distribution level, iii) millisecond-level precise distribution generation control, and iv) real-time wide-area monitoring in a cross-border scenario. This target is materialized by the introduction of the ambitious concept of NetApps and the development of an open experimental facility supporting their integration, testing and validation by third parties, bringing 5G technologies to the reach of start-ups and new entrants, maximizing their impact in the industry and thus accelerating growth.

This deliverable (D2.2) presents the concept of novel Smart5Grid NetApps, the overall architecture of the Smart5Grid open 5G platform as well as its main user roles and scenarios. It receives the input of D2.1 "Use cases, system requirements and planned demonstrations" [1], the first deliverable submitted by the second Work Package (WP2) of Smart5Grid project, which verses around the elaboration of demonstrator Use Cases (UC), identification of technical requirements, and definition of an Open 5G Platform that will support said UCs.

The Smart5Grid NetApp is conceived as a vertical application, composed by a chain of cloud native Virtual Network Functions (VNFs), able to leverage 5G and edge infrastructure by formally specifying its deployment and performance requirements in a NetApp Descriptor. This document describes this concept and its technical specification, including the progress on the definition of the UC NetApps proposed in D2.1.

For third-party developers and Small- and Medium-sized Enterprises (SMEs) to benefit from the application of NetApps to the energy sector, Smart5Grid proposes to ease the barriers for new entrants to such a critical market by defining an Open 5G Platform that, incorporating Development and Operations (DevOps) practices, allows them the verification and validation of applications and VNFs, not just locally, but in quasi-production environments, before deploying them in real operational conditions, thus increasing their trust on the behaviour of said applications. Besides, these tested NetApps and VNFs can be later shared with other developers and consumers fostering their visibility but also encouraging collaboration and, therefore, innovation.

To realize this, the Smart5Grid Open 5G Platform is defined by three distinct layers. The top layer is composed of: (a) an Open Service Repository (OSR) that stores validated NetApps; (b) a Verification and Validation (V&V) Framework that enables intensive NetApp testing; and (c) a User Interface (UI) that allows the interaction of developers and consumers with the platform. The V&V Framework is supported by a telecommunications and virtualization infrastructure, the second layer of the Smart5Grid 5G Platform, that hosts the deployment of NetApp instances for validation purposes; both the infrastructure and the deployment of NetApps are controlled by a Management and Orchestration (M&O) framework, which includes the systems required to interpret, deploy, and monitor the functions described by the NetApp descriptor across its lifecycle. Finally, we find the energy infrastructure layer, composed of the devices and power equipment that connect to the NetApp services.

Apart from the definition and specification of the NetApp concept and the platform architecture as well as the update on the definition of the UC NetApps, throughout the pages of this deliverable, we can also find

a revision of the state of the art around smart grids, the cloud native paradigm, as well as edge and vertical services, in-depth information regarding the different layers that compose the proposed Smart5Grid architecture, their components, and the interactions between them.

Table of contents

List of figures

List of tables

Notations, abbreviations, and acronyms

Item	Description
3D	Three-Dimensional
3GPP	3rd Generation Partnership Project
4G	4th Generation (of mobile telecommunication networks)
5G	5th Generation (of mobile telecommunication networks)
5GCN	5G Core Network
5G-NR	5G New Radio
5G PPP	5G Infrastructure Public Private Partnership
6G	6th Generation (of mobile telecommunication networks)
A&A	Authentication and Authorization
AAA	Authentication, Authorization and Accounting
AB	Advisory Board
ACK, ack	Acknowledgment
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access & Mobility Management Function
AMI	Advanced Metering Infrastructure
AN	Access Network
AP	Access Point
API	Application Programming Interface
APN	Access Point Name
APP	Application
AUSF	Authentication Server Function
AWS	Amazon Web Services
BIOS	Basic Input/Output System
BRP	Balancing Responsible Party
BSP	Balancing Service Provider
BSS	Battery Storage System
BSS	Business Support System
BBU	Base Band Unit
CA	Consortium Agreement
CAPIF	Common API Framework
CFS	Customer Facing Services
CIR	Container Image Registry
CISM	Container Infrastructure Service Management
CFS	Customer Facing Service
CLI	Command Line Interface
CM	Configuration Management

Item	Description
CoE	Centre of Excellence
CN	Core Network
CNCF	Cloud Native Computing Foundation
CNF	Cloud Native Foundation
CP	Connection Point
CPD	Connection Point Descriptor
CPE	Customer Premises Equipment
CPF	Control Plane Function
CPU	Central Processing Unit
CT	Current Transformer
CRAN	Cloud RAN
CRUD	Create, Read, Update, Delete
CSMF	Communication Service Management Function
CUPS	Control and User Plane Separation
DCN	Data Communication Network
DER	Distributed Energy Resources
DevOps	Development and Operations
DHCP	Dynamic Host Configuration Protocol
DLT	Distributed Ledger Technology
DN	Data Network
DNAI	Data Network Access Identifier
DNN	Data Network Name
DNP3	Distributed Network Protocol 3
DNS	Domain Name System
DoW	Description of Work
DRAM	Dynamic Random-Access Memory
DRES	Distributed Renewable Energy Sources
DSO	Distribution System Operator
DSS	Dynamic Spectrum Sharing
E2E	End-to-End
EC	European Commission
EDSO	European Distribution System Operators for Smart Grids (non-profit association)
EEGI	European Electricity Grid Initiative
ENTSO-E	European Network of Transmission System Operators for Electricity
EPC	Evolved Packet Core
EPIA	European Photovoltaic Industry Association
ETSI	European Telecommunications Standards Institute
EU	European Union
EWEA	European Wind Energy Association

Item	Description
FM	Fault Management
FP7	Seventh Framework Program
FPS	Frames Per Second
GA	Grant Agreement
GDS	Global Digital Services
GIT	Global Information Tracker
gNB	G NodeB [Next Generation NodeB]
GOOSE	Generic Object-Oriented Substation Even
GPS	Global Positioning System
gRPC	Google Remote Procedure Calls
GUI	Graphical User Interface
HIL	Hardware-in-the Loop
HMI	Human-Machine Interface
HSS	Home Subscriber Server
HTTP(S), https	Hypertext Transfer Protocol (Secure)
HVAC	Heating, Ventilation and Air Conditioning
HW, hw	Hardware
IaaS	Infrastructure-as-a-Service
IAP	Identity and Access Proxy Identity and Access Proxy
ICT	Information and Communications Technologies
ID, id	Identifier
IETE	Internet Engineering Task Force
IMT	Information Model Translation
IoT	Internet of Things
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Secure
iPXE	Preboot eXecution Environment
ISG	Industry Specification Group
ISO	Optical Disc Image
IT	Information Technology
KPI	Key Performance Indicator
LADN	Local Area Data Network
LAN	Local Area Network
LBO	Local Break-Out
LCM	LifeCycle Management
LDAP	Lightweight Directory Access Protocol
LI	Lawful Interception
LTE	Long-Term Evolution
LV	Low Voltage
M2M	Machine-to-Machine

Item	Description
M&O	Management and Orchestration[1]
MANO (NFV)	Management and Orchestration[1]
MCIO	Managed Container Infrastructure Object
MCIOP	Managed Container Infrastructure Object Package
MCM	Machine-Cloud-Machine
MEC	Mobile Edge Computing
MECO	Multi-access Edge Computing Orchestrator
ML	Machine Learning
MME	Mobility Management Entity
MMS	Manufacturing Message Specification
mMTC	Massive Machine Type Communications
MNO	Mobile Network Operator
MQTT	Message Queuing Telemetry Transport
MSA	Micro-Service Architecture
MTC	Machine Type Communication
MV	Medium Voltage
NAS	Non-Access Stratum
NB	Northbound
NBI	Northbound Interface
NBC IM	Nearby Computing Information Model
NetApps	Network Applications
NEF	Network Exposure Function
NETCONF	Network Configuration Protocol
NF	Network Function
NFD	Node Feature Discovery
NFMF	Network Function Management Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVIaaS	NFV Infrastructure-as-a-Service
NFVO	Network Function Virtualization Orchestrator
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology
NR	New Radio
NRF	Network Repository Function
NRF	Network Resource Function
NS	Network Service
NSaaS	Network Slice-as-a-Service

[1] Through this deliverable, "Management & Orchestration" is abbreviated as MANO (or NFV MANO) when referring to the Management and Orchestration as defined by ETSI NFV [61], and M&O when referring to the Management and Orchestration framework of the NFV/TELCO layer of the Smart5Grid Architecture (Section 4.4)

Item	Description
NSD	Network Service Descriptor
NSFVal	Network Services and Functions Validator
NSI	Network Slice Instance
NSMF	Network Slice Management Function
NSO	Network Service Orchestration
NSSAAF	Network Slice-Specific Authentication and Authorization Function
NSSI	Network Slice Subnet Instances
NSSF	Network Slice Selection Function
NSSMF	Network Slice Subnet Management Function
NWDAF	Network Data Analytics Function
nZTP	near Zero-Touch Provisioning
O-RAN	Open-RAN
OAM	Operations, Administration, and Management
ONAP	Open Network Automation Platform
OPC	Open Platform Communications
OS	Operating System
OSM	Open-Source Mano
OSR	Open Service Repository
OSS	Operational Support Systems
PaaS	Platform as a Service
PAS IEC	Publicly Available Specification
PC	Personal Computer
PCF	Policy Control Function
PDC	Phasor Data Concentrator
PDN	Packet Data Network
PFD	Packet Flow Description
PGW	Packet Data Network Gateway
PM	Performance Management
PMU	Phasor Measurement Unit
PNF	Physical Network Function
PoP	Points-of-Presence
PPDR	Public Protection and Disaster Relief
PSB	Program Specific Block
PST	Power System Testbed
PV	Photovoltaics
QoS	Quality of Service
RAN	Radio Access Network
RES	Renewable Energy Sources
REST	Representational State Transfer
RO	Resource Orchestrator
RoCoF	Rate of Change of Frequency

Item	Description
ROS	Robotics Operating System
RSC	Regional Security Coordinator
RSU	Road-Side Units
RT	Real-Time
RTD	Research and Technology Development.
RT-HIL	Real-Time Hardware-In-the Loop
RTLS	Real-Time Location System
RTS	Real-Time Simulator
RTU	Remote Terminal Unit
SAP	Service Access Point
SBA	Service-Based Architecture
SBI	Southbound Interface
SCADA	Supervisory Control and Data Acquisition
SDK	Service Development Kit
SDN	Software-Defined Network
SEAF	Security Anchor Functionality
SEAL	Service Enabler Architecture Layer
SGW	Serving Gateway
SGW-LBO	Serving Gateway with Local Breakout
SHA-1	Secure Hash Algorithm 1
SIEM	Security Information and Event Management
SLI	Service Level Indicator
SLO	Service Level Objective
SM	Slice Manager
SME	Small and Medium Enterprise
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SP	Service Providers
SSH	Secure Shell
SV	Sampled Value
SW, sw	Software
T&D	Transmission and Distribution
T&L	Transport and Logistics
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TN	Transport Network
TPM	Trusted Platform Module
TR	Technical Report
TS	Technical Specification
TSO	Transmission System Operator
UA	Unified Architecture
UC	Use Case

Item	Description
UCY	University of Cyprus
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
UI	Use Interface
UL	Up-link
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
URL	Uniform Resource Locator
URLLC	Ultra-Reliable Low Latency Communications
UUID	Universally Unique Identifier
UWB	Ultra-Wideband
V2G	Vehicle-to-Grid
V2H	Vehicle-to-Home
V2X	Vehicle-to-Everything
V&V	Verification and Validation
VDU	Virtual Deployment Unit
VIM	Virtual Infrastructure Manager
VLD	Virtual Links Descriptor
VM	Virtual Machine
VNF	Virtual Network Function
VNFaaS	Virtual Network Function-as-a-Service
VNFC	Virtual Network Function Component
VNFFG	VNF Forwarding Graph
VNFD	Virtual Network Function Descriptor
VNFM	Virtual Network Function Manager
VDU	Virtual Deployment Unit
VLAN	Virtual Private Network LAN
VLD	Virtual Link Descriptor
VPN	Virtual Private Network
VSB	Vertical Service Blueprint
VSD	Vertical Service Descriptor
vPDC	virtual Phasor Data Concentrator
VPN	Virtual Private Network
VT	Voltage Transformer
WAM	Wide Area Monitoring
WAN	Wide Area Network
WP	Work Package
WWW, www	World Wide Web
ZTP	Zero-Touch Provisioning

Table 0-1 Acronym list

1 Introduction

This deliverable is the second of the series of three WP2 reports to be delivered by the project consortium during its 36-month work plan.

The first report, "*D2.1: Use cases, system requirements and planned demonstrations*" [1], was delivered in month 6 of the Project. It provided an initial description of the UCs design and of their functional and non-functional requirements, as well as the identification of the fundamental limitations addressed, envisaged innovations, and key system requirements.

The main purpose of this second one, "*D2.2: Overall Architecture Design, Technical Specifications and Technology Enablers*", is, as its name suggests, to present the Smart5Grid reference architecture, to provide the technical specifications of each of its main components, and to introduce the technological choices of the project.

The third one, "*D2.3: Alignment with Previous 5G PPP Phases and Roadmap for third party involvement*", to be submitted in month 24 of the project schedule, will include an analysis of the technologies of previous phases of the 5G Public-Private Partnership (5G PPP) and the Smart5Grid positioning, the identification and analysis of parameters that may affect the final commercial adoption, the roadmap for SMEs and third-party experimentation as well as the evaluation strategy.

1.1 Scope of the document

As stated before, D2.2 aims to:

1) Introduce the overall Smart5Grid Open 5G Platform architecture. This includes the definition of all layers, functional description of sub-modules, interfaces, and data to be exchanged.
2) Present the technical specifications and the analysis of new 5G smart grid technological solutions.
3) Provide the definition and specification of the Smart5Grid NetApps.

This deliverable covers the activities performed as part of the "*Task 2.2: Overall Architecture Design of Open Experimental 5G Platform and NetApps Specifications*" and *the "Task 2.3: System Level Technical Specifications and Technological Choices for 5G Enabled Smart Energy Grids"*. These two tasks ran in parallel for the nine first months of the project and were interdependent with T2.1, being active during the first six months. The results of these three tasks have set the basis for the work in the rest of the project´s WPs.

1.2 Relation with D2.1

The content of this deliverable is tightly related to the results presented in D2.1, which defined the four UCs to be implemented by the Smart5Grid project as well as their associated NetApps, listed as follows:

1. Automatic power distribution grid fault detection, whose main objective is the remote connectivity of grid elements for automation and real-time monitoring of the energy distribution network and the verification of the performance improvement. A 5G network will be deployed offering high levels of availability and reliability. The goal is to reduce the effort and time for troubleshooting communication problems between the central hub and the field devices. A NetApp will be developed to perform continuous monitoring of the communication service level, providing the

Distribution System Operator (DSO) with statistics of the Radio Access Network (RAN) service levels in terms of bandwidth and latency.

- Remote inspection of automatically delimited working areas at distribution level, whose purpose is to develop an automated process to detect workers and their tools when accessing a primary power substation. This detection is carried out by ultra-wideband cameras and sensors, which need fast and low latency processing capabilities. As the delimitation of the zones must be in real time, a private 5G network with edge computing capabilities will be used. The Real-Time Location System (RTLS) to be developed in the Smart5Grid project will monitor activity and create a 3D volumetric security zone, as well as trigger audio-visual, electronic and physical warnings when required. The NetApp to be created as part of this UC will receive the information collected by the sensors and process it, verifying the data and evaluating them, to activate a danger alert signal in case the workers or their tools are in the danger zone.
- Millisecond level precise distributed generation monitoring has as main objective to accurately monitor, at the millisecond level, the distributed power generation in a wind farm by using the capabilities of 5G networks. This monitoring will be vital, as it will allow cost reductions by controlling and preventing future failures. In addition, accurate and high granularity power control will allow wind farm owners to increase their role as both Balancing Responsible Party (BRP) and Balancing Service Provider (BSP). The NetApp developed in this UC will consist of two components: one in charge of predictive maintenance, reporting sensor measurements to understand the performance of each component; the second component will be responsible for: 1) real-time energy production control, thus increasing the efficiency and accuracy of production control and forecasting; and 2) improving the stability of the electricity system by using data such as meteorological data.
- Real-time Wide Area Monitoring (WAM), with the scope of monitoring in real time a wide geographical area where cross-border energy exchanges take place. In this case, the interconnection flow between Greece and Bulgaria grids will be monitored, using 5G infrastructure and executed from the Regional Security Coordinator (RSC) of Greece. Phasor Measurement Units (PMU) will monitor this interconnection and interface with a virtual Phasor Data Concentrator (vPDC) that will be developed to collect the data. The 5G network will improve the connectivity of these PMUs to the vPDC by providing low latency and high reliability. This UC´s NetApp consists of three services: the first service is a vPDC in charge of collecting data from the PMUs and synchronising the measurements according to their time stamp; the second component is the WAM service in charge of status indicators and visualisation features of the PMUs, such as a map indicating the current location of the device; and the third component is the advisory service in charge of proposing corrective actions for real-time operation to both Transmission System Operators (TSOs) and the provision of ex-post analysis in case of severe energy network events.

D2.1 also provided the functional and non-functional requirements of the Smart5Grid project´s architecture. Both the design and needs of the four uses cases and well as the initial requirements presented in D2.1 were taken into consideration in this deliverable to:

- Present the Smart5Grid NetApp concept.
- Define the Smart5Grid architecture, with its three different layers.
- Provide the technical specification of the components that comprise each of these layers.

- Specify the Smart5Grid NetApp descriptor.

1.3 Document structure

The deliverable is organized in the following manner:

- Section 1 (this section) is an introduction to the deliverable.
- Section 2 includes the state of the art and other initiatives in the context of the project.
- Section 3 introduces the Smart5Grid NetApp concept, presents the Smart5Grid open experimental platform architecture, and identifies its different user roles and scenarios.
- In Section 4, the technical specifications and technology enablers are presented.
- The specification of the UC individual Smart5Grid NetApps is included in Section 5.
- Finally, Section 5.4.4 provides conclusions and next steps.

2 State of the art and alignment with other 5GPPP Initiatives

Smart5Grid constitutes a step forward in the integration of energy grids with the latest innovations in virtualization and communication technologies that 5G, the 5th Generation of mobile communications, brings. This section takes a deep dive in the state of the art from the project´s perspective, providing insights on the latest advancements in areas such as smart grids, the cloud native paradigm, the impact of edge computing in 5G networks, etc. It also includes a review of other 5G PPP projects that tackle the topic of vertical applications.

2.1 Smart Energy Grids

Energy market context

The profound transformation driven by deeper and faster decarbonisation is changing the energy world and is also creating new challenges, both on the supply side and on the demand side. The power sector is strongly involved in the process and will deliver a significant part of the necessary efforts. In this context, the energy infrastructure needs to be enhanced and digitalized in order to cope with the deployment of renewable sources, increased decentralization, electrification of end-user and active customers, ensuring, at the same time, energy network stability, security, and resilience.

Electricity generated from renewable sources is predominantly variable in nature; in this respect, grids will be required to manage power flows more promptly and efficiently to support the integration of less predictable energy production, while maintaining the quality of supply. Nonetheless, supporting the boost of Renewable Energy Sources (RESs), smart grids will deliver substantial benefits in terms of resource-efficient economic growth, global and local pollution reduction.

Grid interoperability with distributed resources – including small Photovoltaic (PV) and storage, energy communities and 'prosumers' – is one of the fundamental pillars of grids' development. Shifting from demand and supply patterns toward more decentralized generation (connected at medium and low voltage grids) raises the need to properly manage congestions and multidirectional energy flows. Moreover, connecting customers equipped with smart meters to the distribution system will allow their active participation to the energy market through the provision of flexibility services (demand response[2]).

Energy consumption patterns are changing too, due to the growth of new forms of energy demand in building, transport, and industry sectors, with a high variability and high-power rating – such as charging of electric vehicles, heat-pumps, and other spreading consumer-based devices. The smart integration of electricity with final uses will significantly decrease both greenhouse gas emissions and energy demand, in order to deliver equivalent services with less energy input and resources.

[2] Demand response is a change in the power consumption of an electric utility customer to "better match" the demand for power with the supply. Until recently, electric energy could not be easily stored, so utilities have traditionally matched demand and supply by throttling the production rate of their power plants, taking generating units on or off line, or importing power from other utilities. There are limits to what can be achieved on the supply side, because some generating units can take a long time to come up to full power, some units may be very expensive to operate, and demand can at times be greater than the capacity of all the available power plants put together. Demand response seeks to adjust the demand for power instead of adjusting the supply.

Energy system operators will have to be empowered with more advanced instruments to provide reliable electricity supply and quality of service in the increasing challenging energy system. The goal is to allow the grid system to work as efficiently as possible, minimizing operating costs and environmental impacts while maximizing system stability and security. This is key to ensure more resilient supply of electricity – with raising relevance in a scenario where climate change poses a major risk for infrastructure – through the use of solutions that improve fault detection and allow self-healing of the energy distribution grid, without the intervention of technician.

Smart grids accomplish the required optimization of energy networks by using digital and other advanced technologies. They are necessary for the integration of growing amounts of variable RESs (like solar and wind power), and of new loads (such as energy storage and charging of electric vehicles), while maintaining stability and efficiency of the system. Furthermore, smart grids enable the utilization of flexibilities[3] that are currently available or that will become available in the future, to better match needs on the grid with respect to generation and demand.

On this regard, Smart5Grid platform aims to support the energy transition by providing the needed digital layer to ensure the availability of the communication infrastructure, whenever is needed.

Main functionalities of Smart Grids

Smart grids are complex systems which offer "more than simply the sum of the constituent parts". With respect to power transmission and distribution networks, smart grids integrate interconnected and geographically wide distributed components, both hardware and software, both on the demand and on the supply side, and pool their resources to create higher functionalities such as the following:

[1] Advanced metering and monitoring, for close to real time transmitting and receiving data for information, monitoring, and control purpose on what goes on the energy network, in order to acquire/provide feedback for the grid operation and enable consumers to better manage consumptions.
[2] Active network management, for the operational optimization through predictive maintenance, energy network remote reconfiguration and recovery schemes activation in almost real time.
[3] Flexibility services, from Distributed Energy Resources[4] (DERs) such as distributed generation, energy storage assets and demand side response, leveraging on end-user's flexibility.

[3] Flexibility in the power system is defined as the change in feed-in or withdrawal, in response to an external signal with the aim of providing a service in the power system.
[4] A Distributed Energy Resource (DER) is a small-scale unit of power generation that operates locally and is connected to a larger power grid at the distribution level. DERs include solar panels, small natural gas-fuelled generators, electric vehicles, and controllable loads, such as HVAC (Heating, Ventilation and Air Conditioning) systems and electric water heaters. An important distinction of DER is that the energy it produces is often consumed close to the source.

[4] Smart charging services, such as vehicle-to-grid[5] or vehicle-to-home[6] solutions (for battery electric and plug-in hybrid vehicles) and additional growth of electrification grade (i.e.: heating and cooling), increasing RESs grid hosting capability.

Smart5Grid will support most of those functionalities, offering dedicated services not only for the energy system operators, but also for DERs providers and aggregators, the new emerging actors of the energy industry ecosystem:

- Regarding advanced monitoring, an innovative cross-border frequency monitoring system will be implemented to support the regional TSOs to provide the system stability in the Greek-Bulgarian demo.
- Besides this, in the Spanish demo, an innovative safety system for people working in high-voltage power stations will also be implemented and tested, since electricity still represents a danger for workers if not properly approached, keeping the due physical distance from the live parts.
- The most advanced active grid management system, developed by Enel Distribuzione Italia (EDI), will be supported by a NetApp to provide real-time communication monitoring, preparing the ground for further implementation of edge-based computing.
- The real-time monitoring and control of DERs are the base to provide flexibility services to the energy system operators.

Smart5Grid and NRG-5 5G PPP projects

The energy sector represents undoubtedly one of the most significant "test cases" for 5G enabling technologies. This is linked to the need of addressing a huge range of very diverse requirements to deal with across a variety of applications, like the stringent capacity for smart metering/Advanced Metering Infrastructure[7] (AMI), that is used as a two-way channel for communications between meter and users, versus the latency for supervisory control and fault localization.

Moreover, to effectively support energy utilities along their transition towards more decentralized renewable-oriented systems, there are different open issues to be fully solved as, for example, the need for 5G networks to enable the management of automation, security, resilience, scalability, and portability of the smart grid energy services.

With this aim, the 5G PPP project NRG-5 [3] defined a novel 5G PPP-compliant software framework specifically tailored for the energy domain, which is using: i) trusted, scalable and lock-in free plug-and-play support for a variety of constrained devices; ii) 5G devices' abstractions to demonstrate massive Machine Type Communications [4] (mMTC), and Extended Massive Broad Band communications coupled

[5] Vehicle-to-Grid (V2G) is a technology that enables energy to be pushed back to the power grid from the battery of an electric car. With electric vehicle-to-grid technology – also known as car-to-grid – a car battery can be charged and discharged based on different signals, such as energy production or consumption nearby.

[6] A Vehicle-to-Home (V2H) system enables customers to store home generated renewable energy in their leaf battery, or fill their battery when energy tariffs are low or even free. Customers can then draw energy out to power their home when it is needed or tariffs are high.

[7] AMI provides electric power utilities with a two-way communication system from control centre to the meter, as well as the ability to modify customers' different service-level parameters. The expansion of AMI technologies and developments of smart meter installations through smart metering programs provide distribution grids with a great opportunity to capture voltage feedback of termination points. Here, one important question is how many measurement nodes does energy conservation and optimization solution require.

with partially distributed, trusted, end-to-end (E2E) security; iii) Machine-Cloud-Machine (MCM) communication to enable secure, scalable and energy efficient communications, supporting the notion of virtual device twinning at the edge cloud, iv) an extended Mobile Edge Computing [8] (MEC) infrastructure to reduce backhaul load, increase the overall network capacity and reduce delays, while facilitating the deployment of generic Network Function Virtualisation (NFV) and utility-centric VNFs.

Smart5Grid, although acting in a different area of the power grid than NRG-5 (behind the meter vs after the meter), follows this project in some aspects and completes the NRG IaaS functionalities with the main aim to provide a platform based on chained VNFs, as NRG-5 did.

Smart5Grid's main aim, in fact, is to provide an environment in which it is easy to develop applications for the smart grid, thus abstracting the complexity of the underlying 5G network via the NetApp concept to evolve what has been proposed in NRG-5.

2.2 The cloud native paradigm

Cloud Native concept

In Smart5Grid we will embrace and adopt, where possible, the cloud native paradigm [5]. The concept of cloud native, in a simple way, can be defined as related to applications that are born in the cloud - as opposed to applications that are born and raised on-premises. However, this definition is quite simple and not representative of what cloud native truly means, so it is better to introduce the concept by means of different examples extracted from [6]. Cloud native applications have the following characteristics:

- They often need to operate at global scale. While a simple website can be accessed anywhere given that internet is not blocked, the concept of global implies that the application's data and services are replicated in local data centres so that interaction latencies are minimized, and the integrity of the application is crystal clear to the final user.
- They must scale well with thousands of concurrent users. This is another dimension of parallelism that is orthogonal to the horizontal scaling of data required for global-scale distribution and it requires careful attention to synchronization and consistency in distributed systems.
- They are built on the assumption that infrastructure is fluid and failure is constant so even in the case the failure rate is extremely small, the law of large numbers guarantees that in a global scale even a low probability event can happen.
- Cloud-native applications are designed so that upgrade and test occur seamlessly without disrupting production.

These characteristics perfectly match the requirements of a smart grid's communication and application layers, consequently entailing the need of adopting 5G. Due to the need of addressing a huge range of very diverse requirements to deal with across a variety of applications, an approach based on micro-

[8] Mobile Edge Computing (later also known as multi-access Edge Computing) technology is also being leveraged in 5G. MEC systems "bring" the service close to the network edge, therefore, close to the device's point of attachment. This entity contains the applications and a virtualisation infrastructure which provides compute, storage, and network resources, and also the functions needed by applications.

services and cloud nativeness is strongly needed with the consequent use of different techniques of virtualization, to help the power grid to truly become smart.

The current specifications for realizing network virtualization and softwarization in 5G change how network functions are realized and deployed (as software instances hosted on Virtual Machines[9] (VMs) and/or containers[10]) but not with regards to how the functions are designed. In fact, the state of the art of [11] NFV implementations often replace monolithic hardware-based network functions with their monolithic software VNF counterparts. This approach naturally brings for any project based on software virtualization to the creation of a certain number of common functionalities that are repeated across different VNFs, and which causes evident repetition and lack of flexibility in the network infrastructure. Moreover, NFV and Software-Defined Network[12] (SDN) architectures both comprise a set of predefined function blocks that are interconnected via standardized reference points so, whenever a new function block is added into the architecture, these features bring a further ossification of the network infrastructure[13].

A promising way to tackle this problem with the current NFV and SDN architectures is to enable finer granularity for network functions and a common interface for loose-coupling interaction among them. The Service-Oriented Architecture (SOA) [7], with its latest development as the Micro-Service Architecture (MSA), offers an effective approach to achieve this objective[14]. In the European Telecommunications Standards Institute (ETSI) NFV specifications, a network service refers to an ordered set of (virtual) network functions specified by a service description (VNF forwarding graph [8]). In the SOA approach, this principle

[9] In computing, a Virtual Machine (VM) is the virtualization/emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

[10] A data container is a data structure that "stores and organizes virtual objects (a virtual object is a self-contained entity that consists of both data and procedures to manipulate the data).

[11] NFV is a paradigm shift in how the networks that underpin today's service provider infrastructures are built and operated, and how the services they deliver are managed. New degrees of freedom are introduced to the network and its management as resources now may be added, changed, and removed dynamically. This change opens up a wave of new business opportunities. However, a new and highly agile operational approach is needed to take full advantage of these opportunities.

[12] Another new feature of 5G networks is what is called SDN which provides the separation of the control plane from the user plane. The usage of SDN allows for a high level of programmability, enabling the separation of the network in different slices within the same hardware. Each slice can then be dedicated to a different type of service. SDN is a complementary trend to NFV that allows the control of network resources to be opened to third parties, with the possibility for these third parties to manage their own physical or virtual resources individually, as needed, with the required level of performance tailored to actual needs. SDN centrally configures and manages physical and virtual network devices in datacentres, such as routers, switches, and gateways. For further information also see:, for example: Li, Y., and Chen, M. (2015). Software-defined network function virtualization: A survey. IEEE Access, 3, 2542-2553.

[13] The combination of NFV and SDN technologies enables a lower capex as compared to traditional networks, accelerating time to market. For more details see, for example: Nguyen, V.-G., Brunstrom, A., Grinnemo, K.-J., and Taheri, J. (3rd quart. of 2017):.SDN/NFV-based mobile packet core network architectures: A survey. *I*EEE Communications Surveys and Tutorials, 19(3), 1567-1602.

[14] The Service-Oriented Architecture (SOA) is an architectural style that supports service orientation. By consequence, it is as well applied in the field of software design where services are provided to the other components by application components, through a communication protocol over a network. More details can be found, for example, at: https://en.wikipedia.org/wiki/Service-oriented_architecture. The Micro-Service Architecture (MSA) enables the rapid, frequent and reliable delivery of large, complex applications. It also enables an organization to evolve its technology stack. More informative details can be found, for example, at: https://microservices.io/

has been embraced by the NFV architecture in different level as NFVIaaS [9], VNFaaS [10], and NSaaS [11], which all adopt the SOA service concept, as specified in [12].

The application of the virtualization and service-oriented principles in network design enables network systems to be realized based on cloud technologies and network services to be provisioned following the cloud service model [13]. This emerging trend is often referred to as cloud native network design, which is expected to be widely adopted in future networks, including the design of 5G/6G networks. Cloud native is an approach to design, build and run applications/virtual functions that fully exploits the benefits of the cloud computing model. It refers to the way applications are created and deployed, not where they are executed, and it is based on the principle of decomposing an application into a set of microservices that can be developed and deployed independently to accelerate and optimize the DevOps strategies. The microservices are packaged into light-weight containers which are scheduled to run on compute nodes by a container orchestrator. As regards data, we must underline that, to be properly classified as cloud native, microservices need to be "stateless", meaning that there must be a separation of the processing logic from the processed data and how it is stored in the cloud

In Smart5Grid we will embrace and adopt where possible the cloud native paradigm to pave the way towards the integration of the energy infrastructure and the 5G Core Network (CN) SBA[15]. This 5G CN SBA will require several techniques being applied in unison, i.e., NFV and SDN that will require the deconstruction of VNFs into microservices. This effectively translates to the containerization of the 5G Core, and the gradual decoupling of network functions from VMs in support of containerized network functions. For this reason, the adoption in the early stage of a cloud native approach for the NetApp development will increase the compatibility between telco and vertical infrastructure.

Cloud Native VNF modelling

In order to understand the road map of the evolution of the VNFs towards a cloud native approach, we can rely on the 5G PPP "Cloud Native and 5G Verticals' services" White Paper [14], that conveys the point of view of the European Commission (EC) and the industry in Figure 2-1.

Figure 2-1 shows the evolution from the classic solution based on VNF implemented to run inside VMs. It also depicts a possible evolution of the term VNF to CNF (Cloud Native Function[16]) that is another way to indicate VNF but with strong emphasis on the cloud design.

Observing the present phase, we can see that the classic solution is based on running VMs on top of bare metal/public cloud and on the use of hypervisors such as VMware [15] or VirtualBox [16]. At the same time, OpenStack [17] has been used as the de facto cloud computing platform. This architectural approach adopted in the Telecom sector follows the NFV MANO [18] (Management and Orchestration) specification.

[15] The 3GPP defines a Service-Based Architecture (SBA), whereby the control plane functionality and common data repositories of a 5G network are delivered by way of a set of interconnected Network Functions (NFs), each with authorization to access each other's services.

[16] A Cloud-Native Network Function (CNF) is a software-implementation of a network function, which runs inside a Linux container (typically Kubernetes), which would traditionally be performed by a physical device. Cloud-Native Network Functions are a successor to Virtualized Network Functions, one of the components of Network Function Virtualization.

This early-stage approach brought many problems. For example, in multi-domain orchestration environments, as the ones used commonly in 5G services, the management of several Virtual Infrastructure Managers (VIM) (e.g.: OpenStack) in a multi-cloud environment is a complex and hard task not easy to solve. Another problem is that it is difficult to manage multiple VNFs in a consistent way because we are facing the hard dependency between the hardware and element management systems that exist in the real environments. Finally, at implementation level, it is also hard to combine different blocks from different vendors. These concerns can be solved if we move forward into a cloud native solution given their foundation principles.

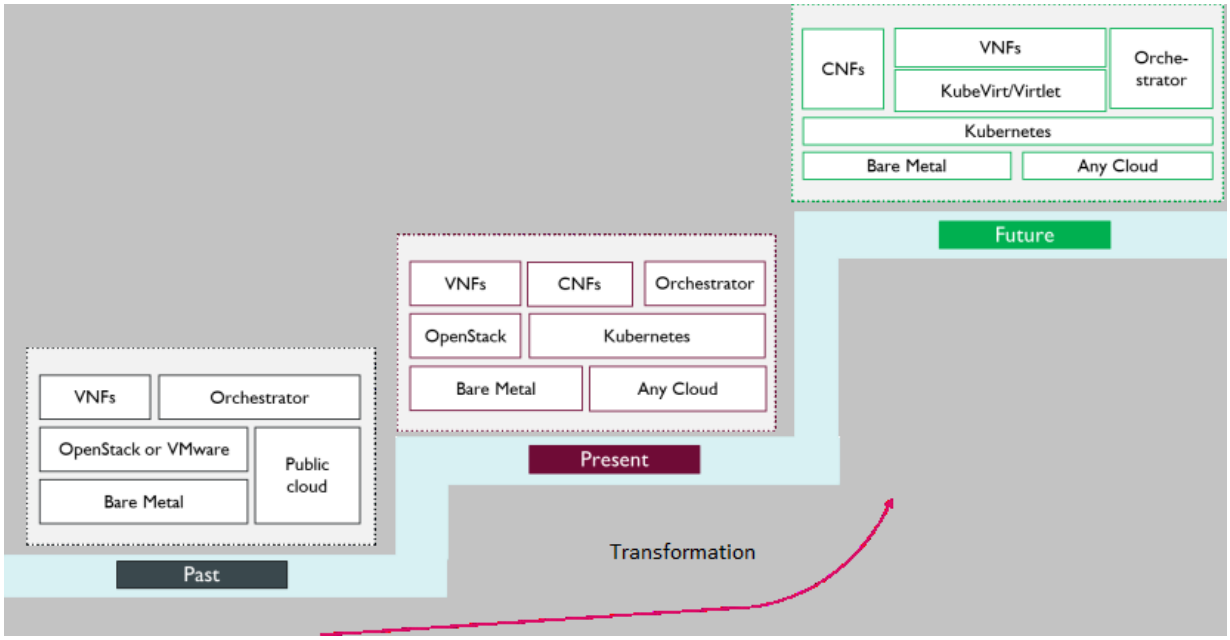

Figure 2-1 Cloud Native Road Path [14]

Summarizing, we can extract four key ingredients that have to guide Smart5Grid project towards the development of cloud native applications. We need:

1) Small, stateless microservices architecture, running in containers, which are faster to get deployed and upgraded with the use of few cloud resources, with the purpose of deploying just what is needed instead of the entire network function.

2) Open architecture and Application Programming Interfaces (APIs) so it is possible to continuously onboard innovation. For example, the 5G core uses an SBA with well-defined APIs for network functions to offer services or call on each other. This, merged with the cloud-native service mesh, enables rapid manipulation of the 5G core, allowing the integration of new network functions, or rapidly scaling & deploying different slices.

3) Cloud agnostic and infrastructure agnostic, to eliminate the hardware dependencies.

4) DevOps for automation and fast time to market.

Cloud native standardization efforts

Regarding standardization efforts, the ETSI NFV group has recently published a report [19], which introduces container-based VNFs covering the following features:

- NFV Architecture support for VNFs which follow cloud native design principles.
- Enhanced NFV MANO capabilities to support container technologies based on DGR/NFV-IFA029 [21].
- Enhanced NFV MANO capabilities for container management and orchestration.
- Enhanced information model for containerized VNFs both using bare metal [17] or nested virtualization[18] technologies.

These features regard SBA design for NFV, VNF generic Operations, Administration, and Management (OAM) functions, as well as enablers for autonomous management in NFV MANO.

The normative work in Release 4 of the NFV framework enhances the support for container-based deployment of VNFs addressing service interfaces for OS (Operating System) container management and orchestration, as well as the requirements for the management and orchestration of container cluster nodes. A better setting for the applicability of current network cloudification trends to NFV is needed, as well as new tools to make network deployments of the operation more automatic and simpler.

Also important in 2020 was the release of the 5G PPP Software Networks Working Group White Paper [14] where the value and challenges of becoming cloud native for the verticals is examined.

As regards the industry, the recent surge of interest in containers, SOA and MSA, as well as orchestration related topics, is fuelled by the need for industry developers to share applications that will scale and run in a consistent manner across many different environments. The need of standardization of such a disruptive environment with a rapidly changing ecosystem has encouraged the creation of the Cloud Native Computing Foundation [20] (CNCF) from the Linux foundation, whose main aim is to serve as the vendor-neutral home for many of the fastest-growing open-source projects related to the cloud native approach.

2.3 Edge Computing and 5G

Edge computing concept

Edge computing refers to a broad set of techniques designed to move computing and storage out of the remote cloud (public or private) and closer to the source of data. Edge computing, as an evolution of cloud computing, brings application hosting from centralized data centres down to the network edge, closer to consumers and the data generated by applications. It is acknowledged as one of the "key pillars" for meeting the demanding Key Performance Indicators (KPIs) of 5G, especially as far as low latency and bandwidth efficiency are concerned. However, Multi-access Edge Computing (MEC) is not only a technical enabler for the demanding KPIs of the telecommunications networks; it also plays an essential role in the transformation of the telecommunications business, where telecommunications networks are turning into versatile service platforms for industry and other specific customer segments. This transformation is

[17] The term "bare metal" refers to the fact that there is no operating system between the virtualization software and the hardware. The virtualization software resides on the "bare metal" or the hard disk of the hardware, where the operating system is usually installed.

[18] Nested virtualization is a complex process that involves running virtual machines within virtual machines. This process is made possible through the use of hypervisors, which are specialized software programs that manage the operating systems needed within virtual environments.

supported by MEC, as it "opens" the network edge for applications and services, including those offered by third parties.

MEC provides an Information Technology (IT) service environment and cloud-computing capabilities at the edge of the mobile network, within the RAN and near mobile subscribers. The aim is to reduce latency, ensure highly efficient network operation and service delivery, and offer an improved user experience.

Thus, MEC is a natural development in the evolution of mobile base stations and the convergence of IT and telecommunications networking. Based on a virtualized platform, MEC has been early recognized by the European 5G PPP research body as one of the key emerging technologies for 5G networks [22], together with NFV and SDN. In addition to defining more advanced air interface technologies, 5G networks leverage more programmable approaches to software networking and use IT virtualization technology extensively within the telecommunications infrastructure, functions, and applications. MEC thus represents a "key" technology and architectural concept to enable the evolution towards 5G, since it helps advance the transformation of the mobile broadband network into a programmable world and contributes to satisfying the demanding requirements of 5G in terms of expected throughput, latency, scalability, and automation.

MEC is based on a virtualized platform with an approach complementary to NFV. In fact, while NFV is focused on network functions, the MEC framework enables applications running at the edge of the network. The infrastructure that hosts MEC and NFV – or network functions – is quite similar; with the aim of allowing network operators to benefit as much as possible from their investment, it would be beneficial to reuse the infrastructure and infrastructure management of NFV to the largest extent possible, by hosting both VNFs and MEC applications on the same platform. MEC's environment is characterized by low latency, proximity to the end-user, high bandwidth, and real-time insight into radio network information and location awareness. All of this can be translated into value and can create opportunities for both mobile operators, and application and content providers, enabling them to play complementary and profitable roles within their respective business models and allowing them to better monetise the mobile broadband experience.

MEC opens services to consumers and enterprise customers as well as to adjacent industries. It enables a new value chain, numerous business opportunities and a myriad of new UCs across multiple sectors. Related market drivers include business transformation, technology integration and industry collaboration. A wide variety of use cases can be supported for new and innovative markets, such as e-Health, connected vehicles, industry automation, augmented reality, gaming, and IoT (Internet of Things) services [23].

MEC is regarded as a key technology to bring application-oriented capabilities into the heart of a carrier's network, to explore a wide range of new UCs, especially those with low latency requirements. When it comes to deployment, there are many potential scenarios where MEC can "fit" in and these are not limited to 4G or 5G. More specifically, edge presence is viewed as necessary to enable certain UC classes defined for 5G [24].

From a Mobile Network Operator's (MNO) point of view, a major challenge in enabling applications associated with the 5G UCs is the significant investment required to deploy a sufficiently extensive network of edge computing Points-of-Presence (PoPs), so that it becomes attractive to develop applications exploiting the edge processing infrastructure in mind. Moreover, this investment must be made in advance

of applications being ready to take advantage of it; that is, it is an investment in anticipation of future revenue, but without any guaranteed near-term returns. One way to mitigate the significant cost (and risk) of such strategic investment is to bootstrap a MEC deployment to the deployment of a Cloud RAN (CRAN): the cost of providing additional processing power across an already planned pool of centralised processing points (e.g.: a pool of Base Band Units (BBUs)), should be significantly lower than a standalone MEC deployment. Conversely, deployment of a CRAN across generic computing infrastructure (as opposed to dedicated, RAN-optimised hardware) is itself a significant investment for an MNO. In addition to the costs of deploying CRAN processing units themselves, there is the cost of moving towards virtualised RAN appliances, testing, integration, and maintenance of these new solutions. While the operational flexibility and network re-configurability offered by virtualisation may carry significant long-term benefits, the near-term effort and costs can make it difficult for adoption. The significant strategic benefits of MEC can make the decision a much clearer one. The ETSI ISG MEC (Industry Specification Group for Multi-access Edge Computing) focuses on enabling edge computing at the access network (mobile or otherwise), thus bringing edge computing as close as possible to the user without it being in the user device[19]. The group has already published a set of specifications (Phase 1) focusing on management and orchestration of MEC applications ([25],[26]), application enablement API [26], service APIs ([27],[28],[29],[30],[31]) and the User Equipment (UE) application API [32]. The management and orchestration, and application enablement functions contribute to enabling service environments in edge data centres, while the service APIs enable the exposure of underlying network information and capabilities to applications. One of the key value-adding features of the MEC specification is the ability for applications to gain contextual information and real-time awareness of their local environment through these standardised APIs. This local services' environment is a flexible and extendable framework, as new services can be introduced by following the API guidelines [33], when creating new service APIs. Last but not least, the UE application API lets the client application in the UE interact with the MEC system for application lifecycle management (LCM). 5G networks based on the 3rd Generation Partnership Project (3GPP) 5G specifications have become a key future target environment for MEC deployments. In addition, the 3GPP 5G system specifications define the enablers for edge computing, allowing a MEC system and a 5G system to collaboratively interact in traffic routing and policy control related operations. MEC features together with complementary technical enablers of the 5G system can allow integration of these systems to create of a powerful environment for edge computing.

Nevertheless, starting from the fact that the MEC's original target was the mobile network, when it comes to its deployment, MEC is often considered as a 5G-only feature. In fact, the MEC reference architecture, defined in ETSI GS MEC 003 [34], is agnostic to the mobile network evolution, so that a MEC host deployed in a 4G network can be reused to support 5G services as well.

Therefore, understanding the impact of deploying an ETSI MEC system into 5G systems is crucial for MNO in order to carefully plan their network upgrades. This way, MEC can be not only a technology ready for 4G, but also a major "driver" to motivate 5G adoption as it can allow operators to retain the prior investment made in 4G deployment. Indeed, from a mobile evolution perspective, products based on

[19] The group was established in September 2014 to standardize APIs enabling application and content providers to utilise computing capabilities present at the edge of the network. MEC enables successful deployment of new use cases like augmented reality, connected vehicles, etc., while various services can be customised according to the customer requirements and demands.

current MEC specifications can be smoothly migrated to support 5G networks through software update. This way, flexibility in the deployment architecture allows planning for the introduction of MEC services as the milestone to build the edge cloud, which is key for the success of 5G services such as URLLC (Ultra-Reliable Low Latency Communications). In Annex A: MEC Framework, we briefly present MEC framework and Mobile Edge System reference architecture, both according to ETSI GS MEC 003.

MEC as a "Driver" to 5G Adoption

MEC makes no assumptions on the underlying radio infrastructure, which makes it a highly flexible element in the communications networks. As the delivery technology – together with the underlying hardware of the MEC platform – remains open, this enables new levels of adaptability to the chosen deployment scenario. Therefore, Service Providers (SPs) can use MEC as a revenue generator and application test bed (including service producing applications) without being forced to wait for full ratification/deployment of the 5G standard and the associated capital investment. This approach allows SPs to offer third parties a cost-effective way to trial their applications. Using an "edge cloud", SPs can host applications in a virtual retail space, test the revenue return, and scale-up or remove as appropriate. So, starting out as a 4G edge test bed with limited deployments at first, MEC allows a smooth transition into the 5G network rollout, removing the need for major upgrades when the expected time for transition arrives.

Another focus area for transitioning from today's 4G to 5G networks is about re-using the existing deployed systems in the process. Due to the MEC's virtualised characteristics, it has never been easier to monitor performance and resource needs of an application which, in turn, enables more accurate pricing for operators towards application providers for hosting the applications.

The common feature set of providing much-improved capabilities at the edge of the network, improved intelligence about resources needed at the edge and the ability to charge for service delivered by cycles, memory, storage, and bandwidth delivered, makes it "quite attractive" to start the deployment in (early) 5G test sites. Taking into account the above considerations, MEC compatibility towards 5G networks may involve:

- Integrating the MEC data plane with the 5G system's one for routing traffic to the local data network and steering to an application.
- An Application Function (AF) interacting with 5G Control Plane Functions (CPFs) to influence traffic routing and steering, acquire 5G network capability information, and support application instance mobility.
- The possibility of reusing the edge computing resources and managing/orchestrating applications and/or 5G network functions, while MEC still orchestrates the application services (chaining).

MEC, as it is deployed in the 4th-generation LTE (Long-Term Evolution) networks, is connected to the user plane. With LTE networks already having been deployed for a number of years, it was necessary to design the MEC solution as an add-on to a 4G network in order to offer services in the edge. Consequently, the MEC system – as defined in ETSI GS MEC 003 [34] and in the related interface specifications – is to a large extent self-contained, covering everything from management and orchestration down to interactions with the data plane for steering specific traffic flows. With 5G, the starting point is different, as edge computing is identified as one of the key technologies required to support low latency together with mission critical and future IoT services, and to enable enhanced performance and quality of experience. The design approach taken by 3GPP allowed the mapping of MEC onto AFs that can use the services and information

offered by other 3GPP network functions based on the configured policies. In addition, a number of enabling functionalities can provide flexible support for different deployments of MEC.

Integration of 5G management, control, and orchestration processes

There is a growing consensus that in the long term, 5G deployments will increasingly integrate fixed-mobile networks infrastructures with cloud computing and MEC. In these scenarios, the borders between cloud and MEC virtual resources will not be explicit, thus paving the way towards a sort of "continuum" of logical resources and functions, offering flexibility and programmability through global automated operations. This will require that the orchestration capabilities, which are already a key element for exploiting cloud computing capabilities, become an essential part of the operation of future 5G infrastructure.

The integration of 5G management, control and orchestration processes is expected to facilitate applications/services development by providing controlled access to high-level abstractions of 5G resources (e.g., abstractions of computing, memory/storage, and networking) thus enabling any vertical application. Moreover, as a real operating system, it should provide automated resource management, scheduling process placement, facilitating inter-process communication, and simplifying installation and management of distributed functions and services, spanning from cloud computing to MEC. This implies a shared data structure capable of supporting multi-vendor systems and applications.

In the specific Smart5Grid framework, the core aim is to focus on the deployment of several selected UCs of strong market relevance for revolutionising the energy vertical industry, in parallel with the introduction of an open 5G experimental facility being able to support integration, testing and validation of existing and new 5G services and NetApps from third parties.

MEC reduces latency to milliseconds and allows for constant connectivity. Plus, when the edge network experiences high traffic, the edge may offload data to the cloud to maintain a quick and reliable connection. Within this environment, MEC can provide a multiplicity of explicit benefits for the provision of the related services to any participating market actor – especially to network operators – and also to support the effective transition towards a reliable 5G implementation.

2.4 Alignment with other 5G PPP projects

Many vertical trials have been performed through the 5G PPP [35], which is now in its third phase, since its launch. The 5G PPP is delivering solutions, architectures, technologies, and standards for the ubiquitous next generation communication infrastructures of the coming decade. The challenge for the 5G PPP is to secure Europe's leadership in the particular areas where Europe is strong or where there is potential for creating new markets.

The 5G PPP Initiative has provided a number of scientific solutions that have been contributed to standardization activities and also the global academic and research community through publications. In addition, the 5G PPP projects have been driving test and validation activities in Europe, collecting significant experience for all stakeholders, and raising public awareness on the capabilities of 5G networks.

As 5G networks are slowly becoming a reality, there is still a further degree of maturity that needs to be reached in order to fulfil on the promises of ubiquitousness and cross industry revolution made by the 5G vision. One of the current hurdles that can be observed in this process, letting aside the search for a killer

application, is precisely the noticeable difficulties on reconciling the expertise across multiple knowledge domains, such as, for example, the Telco and Energy industries.

NetApps and Vertical Applications

Taking on the challenges of ICT-41-2020 [36], Smart5Grid aims to map the requirements of vertical industries, specifically the Energy sector, into software applications that leverage the capabilities of 5G networks to address a vertical demand.

Several 5GPPP projects have tackled in recent initiatives the challenge of easing the adoption of 5G technologies for vertical applications:

5G-TRANSFORMER [37] proposes an architecture where vertical applications can be defined by selecting from a set of Vertical Service Blueprints (VSB), available from a catalogue, and which are tailored to the specific needs of the vertical business. By providing instantiation parameters, these blueprints are then particularized into Vertical Service Descriptors (VSD). The VSDs are used to generate Network Service Descriptors (NSD) that can be used to create an instance of the vertical service.

MATILDA [38] aimed at providing software developers with the necessary tools to develop vertical applications as 5G-ready applications. For this, metamodels were proposed to define two main components of 5G-ready applications, namely: i) chainable application component, which contains details of its requirements such as resources, Quality of Service (QoS), etc.; and ii) the application graph which defines the relations between these application components.

Smart5Grid aims to progress on these two ideas, extending the concept of vertical applications by defining a NetApp. These NetApps implement and package vertical applications, and are formed by a set of VNFs interconnected together. The NetApp concept improves the vertical application by the specification of performance requirements that define how an application leverages edge deployments and how it connects and interacts with the 5G networks.

Including Smart5Grid, the 5G PPP projects funded under ICT-41-2020 propose NetApps as solutions to vertical challenges. The common denominator of this grant is to enable experimentation facilities that help open new markets within the verticals and ease the entrance to these markets for application developers, creating an ideal environment for SMEs and an excellent breeding ground for start-ups in the European ecosystem. The projects participating in this programme are summarized below:

- 5GASP [39]: Netapp test and validation in an open, integrated environment of 5G experimental testbeds with the focus on Automotive and Public Protection and Disaster Relief (PPDR), leveraging on a unified platform that will integrate DevOps practices within its offer capabilities. 5GASP´s NetApp is conceived as a service to verticals, architected following SBA approach using either VMs or cloud-native solutions, and it proposes to align with 3GPP standards such as CAPIF [40] or SEAL [41].
- 5G-EPICENTRE [42] [43]: The project aims to provide an open experimentation platform based on 5G, cloud-native paradigms and DevOps principles. 5G-EPICENTRE also focuses on the implementation of NetApps, to service public security UC, chaining with VM-based VNFs or chaining with cloud-native VNFs. This implementation is facilitated in this project thanks to the NetApps creation and management panel (nappD) allowing the creation of new NetApps, adapting them according to the needs.

- 5G-ERA [44]: The proposed experimentation platform integrates existing testbeds with robotics by adopting widely spread Robotics Operating System (ROS) into their validation process. The project NetApps address UCs from four verticals, Industry 4.0, Transport & Logistics, Public Safety, and eHealth & Wellness, validated across three experimentation facilities.
- 5G-IANA [45]: The project revolves around the Automotive sector and it will offer 3rd party experimenters the necessary software tools and infrastructure to develop NetApps that can reuse Automotive-related VNFs from a repository that will be available to SMEs.
- 5G-INDUCE [46]: The project plans to offer NetApp developers the ability to test and validate their Industry 4.0 applications on a 5G experimentation platform, as well as creating marketplaces for third parties such as SMEs and start-ups. This NetApps development and deployment will showcase support for a variety of innovative Industry 4.0 market verticals through the demonstration of advanced use cases that meet demanding Industry 4.0 and 5G KPIs such as ultra-low latency, rapid service deployment and high service reliability.
- 5GMediaHUB [47]: The consortium's main objective is to allow 3rd party experimenters and NetApp developers to validate media-oriented applications in two testbeds, through an experimentation environment with the aim of supporting a faster adoption of the applications in operational networks. At 5GMediaHUB, NetApps are application enablement services that provide a set of open standard Northbound APIs through which Platform-as-a-Service (PaaS) is offered. The 5GMediaHUB NetApps will be VNF chains within a network subnet instance, aligning with 3GPP TR 28.801 [48] and ETSI NFV.
- EVOLVED-5G [49]: This project takes on the challenge of addressing the Factory of the Future UCs. Its platform will host a marketplace of NetApps that the manufacturing industry can reuse when designing and implementing their applications. Vertical industries will be able to build their own NetApps, i.e.: they will compose services by consuming 3GPP APIs as well as other telco assets. An example of the work that a NetApp could do would be to consume APIs that provide monitoring and analysis of the configuration of network slices to provide quality services.
- VITAL-5G [50]: Transport and logistics is the focus area of VITAL-5G. This project will offer specific and agnostic NetApps that will be validated in real T&L scenarios by supporting open-source tools and an open repository. The validated NetApps, by interfacing with the 5G network, hide their inherent complexity, allowing third parties to develop innovative solutions around them more easily and quickly.

Smart5Grid 5G Experimental Platform aims to provide an experimentation environment for 3rd party developers to implement, verify and validate energy vertical applications as NetApps, composed of a chain of VNFs. These applications, once validated, will be hosted and accessible from an Open NetApp repository, encouraging the reutilization of VNFs and fostering the introduction into the market of start-ups and SMEs.

Smart5Grid´s intention is to collaborate with the other projects under ICT-41-2020 grant, aligning with them, finding commonalities, and mutually benefiting from the advantage of potential synergies. More specifically, Task 2.4 will focus on this alignment with the outcomes of previous 5G PPP phases as well as, later in the project, with those resulting from the collaboration with more recent projects. Also, from Smart5Grid´s WP7, Task 7.3 will ensure a strong European alignment by participating in the different 5G PPP WGs and other relevant 5G fora.

Open Service Repository (OSR)

The Smart5Grid project aims at providing a well-structured way to store, describe and share the developed NetApps and VNFs. Existing technologies have solved the problem of storing and maintaining software code. The OSR platform, along with the User Interface (UI), leverages these technologies to create a tool that offers an intuitive way of developing new NetApps and VNFs with application in the energy domain. It also aids the collaboration between interested parties (SMEs, developers, other 5G-PPP projects). Moreover, it facilitates their deployment on the Smart5Grid platform for validation and verification purposes while it gives the users great visibility on performed actions.

Other projects implementing similar repositories are:

- 5G-IANA, which focuses on NetApps and VNFs of Automotive-related services;
- 5GMediaHUB, re-usable open-source NetApps repository;
- 5GASP, an open-source software repository, hosting applications on the automotive industry and the PPDR;
- VITAL-5G, a repository NetApps for the transport & logistics (T&L) sector;
- NRG-5 [51] an NFV and VNF repository;
- 5G-VICTORY [52], VNF and PNF repositories;
- MATILDA [38], a VNF repository.

The Smart5Grid OSR stands as a part of a wider set of 5G PPP repositories that all work towards similar goals and could, at a later point, be aggregated under a higher-level platform that could incorporate all developed VNFs and NetApps. The Smart5Grid OSR, proactively, exposes the interfaces that will make integration and interoperability possible with such a platform or other, same-level repositories.

Validation & Verification (V&V)

The Smart5Grid project aims to provide the V&V Platform that will be responsible for the auditing of Smart5Grid NetApps by performing automatic verification and validation of the service to be provided, while monitoring and managing results to help in the NetApp development process. The objectives of this platform are two-fold: first to guarantee that the NetApp is working as intended; and second to accelerate the DevOps of the developer, enabling a continuous improvement of NetApps and its VNFs based on the obtained results, thus achieving a continuous integration and development loop cycle.

In other projects as 5GZORRO, *'Zero-tOuch secuRity and tRust for ubiquitous cOmputing and connectivity in 5G networks'* [53], the main contributions are in software system design, Distributed Ledger Tecnologies (DLTs) & smart contracts, and in the development of the Security and Trust Orchestrator, contributing to 5GZORRO platform's ability to tackle common security and trust requirements. In this project, an automatic service validation toolkit is being used, which can be a case study for the V&V Platform.

In CARAMEL, '*Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles*' [54], a MEC network infrastructure and service orchestration platform are provided, which enable the deployment of services close to the Road-Side Units (RSUs) in order to reduce latency for critical components and improve the user's quality of experience. Despite not being considered a validation tool in the DoW, this project would greatly benefit from an automated service validation tool, particularly in the MEC network during

the development phase of the project, where the updates to the VNFs are continuously happening. It is worth considering the addition of a V&V Platform to the project ecosystem in the near future.

In 5GCity [55], the main contribution was focused on the Vehicle-to-Everything (V2X) UC, having also contributed with the design and implementation of core platform components and the overall neutral hosting business modelling. For Smart5Grid, the platform architecture of 5GCity gives insights on how to connect several assets and monitoring all the information regenerated by each of them.

The project SHIELD, '*Securing Against Intruders and Other Threats Through an NFV-Enabled Environment*' *[56]*, focuses on the architecture specification of SHIELD solution and the SHIELD's VNF Store as well as VNF development tailored for SHIELD's UC needs.

In SELFNET, 'Framework for SELF-organized NETwork management in virtualized and software defined networks' [57], the main contribution was in the implementation of VNF based sensors and actuators (targeting Self-Optimization UC) as well as SELFNET's monitoring framework. This knowledge will re-used in Smart5Grid, improving the definition of the NetApps delivered by the project.

Finally, in SONATA, '*Service Programming and Orchestration for Virtualized Software Networks*' [58], the focus was on the implementation of multiple service development tools (Service Development Kit – SDK – module), including a developer workspace, service projects, service packaging, service validation and the interface with the Service Platform. The Network Services and Functions Validator (NSFVal) tool can be used to validate the syntax, integrity and topology of packages, projects, services, and functions. Its architectural design consists of a core validation engine, responsible for consistency and network analysis, and a plugin-based manager responsible for translating and loading descriptors from multiple information model formats. Started in the scope of SONATA, the NSFVal early development has been improving the validator solution to have more features and to support more information models, such as Open-Source MANO (OSM) [59] and Open Network Automation Platform (ONAP) [60]. NSFVal was also used in SHIELD, SELFNET and 5GCity as a third-party library in order to improve their services store module.

The Smart5Grid V&V Cycle will consist of a set of components supporting the development, validation and verification of NetApp workflows that can be realized over the Smart5Grid platform. Moreover, Smart5Grid will embrace the DevOps paradigm for providing access to the Smart5Grid open platform, thus enabling faster and continuous software delivery, less complexity to manage and faster resolution of potential bugs and problems, thus producing NetApps more reliably and at less time. The proposed DevOps approach of the project will be used for flexible Configuration, Performance, and Fault Management (CM, PM, and FM) in the open Smart5Grid platform. Additionally, DevOps principles will be used to involve engineers, developers, SMEs and third parties for accessing, running, and validating their own energy-oriented network services and applications.

3 Smart5Grid NetApp Specification and Platform Architecture

This chapter presents the architecture proposed and introduces the Smart5Grid NetApps concept as a solution to the requirements captured in the previous Smart5Grid deliverable of WP2, that is the D2.1. These requirements contain valuable information regarding two important factors that have been considered in the design of the system described. These two factors are: i) the proposed UCs, which are representative of the challenges faced by the energy sector; and ii) the requirements of the platform from a service and architectural point of view. This architecture builds on the concepts and solutions resulting from previous initiatives and research as outlined in the state of the art section.

3.1 Smart5Grid NetApps

This section, to introduce this chapter 3, presents the Smart5Grid NetApp proposed as a solution to the needs of Smart5Grid project and its UCs, exposed in deliverable D2.1. As it can be seen in the state of the art of this deliverable (Section 2), current technology status and other 5GPPP projects have been examined to define the NetApp specification as closely as possible based on the concepts reviewed.

The Smart5Grid NetApp provides a means for developers to define vertical applications by interconnecting together new and/or existing pieces of software in the form of VNFs. By splitting the functionality of the NetApp into decoupled VNFs, the reutilization of software functions is encouraged. This, however, is not something that the NetApp brings as a new concept. As described in the state of the art section, ETSI NFV framework [61] describes the reference architecture, information models, and tools required to manage this kind of applications. However, when introducing advanced networking in the picture, such as 5G, this framework on its own requires a high level of expertise from developers, not only from the relevant field of the specific vertical application that is being developed, but also from the field of Telecommunications if the building of End-to-End application is the purpose. With this in mind, the Smart5Grid NetApp concept intends to provide a solution to this problem by abstracting the complexities of network deployment and configuration from the developers of vertical applications.

Smart5Grid proposed NetApp is a cloud-native application. Thus, it is made up of VNFs based on OS containers technology. A Smart5Grid NetApp contains the necessary components to offer a service, as a software application, for the energy vertical, i.e., it is a complete and standalone vertical application. However, this does not imply that the service provided by this vertical application cannot be consumed by other external or legacy applications, e.g., from a north-facing API. Also, as shown in Figure 3-1, a NetApp may directly expose other user interfaces, such as dashboards, open to design decisions made by the developer. As already mentioned, NetApp components can be deployed as container-based VNFs. A NetApp can contain one or more VNFs. By splitting these components whenever possible in the implementation, the NetApp brings the opportunity to take advantage of the cloud/edge infrastructure. An example of this could be, in the case of a NetApp composed by two components (Figure 3-2), that the NetApp function that require low latency input or responses could be placed at the edge of the computing infrastructure, while the other function that may be resource-intensive, not suitable for an edge deployment and not requiring its benefits, should be placed in a cloud datacentre where resources are not constrained.

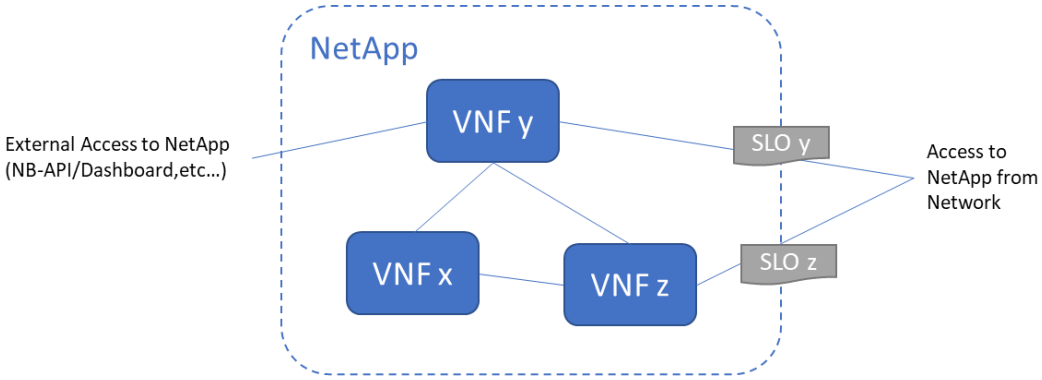

Figure 3-1 Basic NetApp representation

Each NetApp is formally defined in a NetApp descriptor (see Section 4.6) which will include the necessary information regarding the services that compose it, its topology, but also the performance requirements of each component, so that the infrastructure over which it is instantiated can perform their intended functions, such as MEC offloading, VNF scaling, and traffic policy enforcement via its management and orchestration (M&O) systems. This information allows the M&O systems to create end-to-end slices that fulfil these requirements, allowing developers to design applications with strict performance demands without needing the expertise to implement the networks that support them. Future deliverables, in particular D3.1, will explore in more detail the NetApps' full lifecycle managed by the M&O framework.

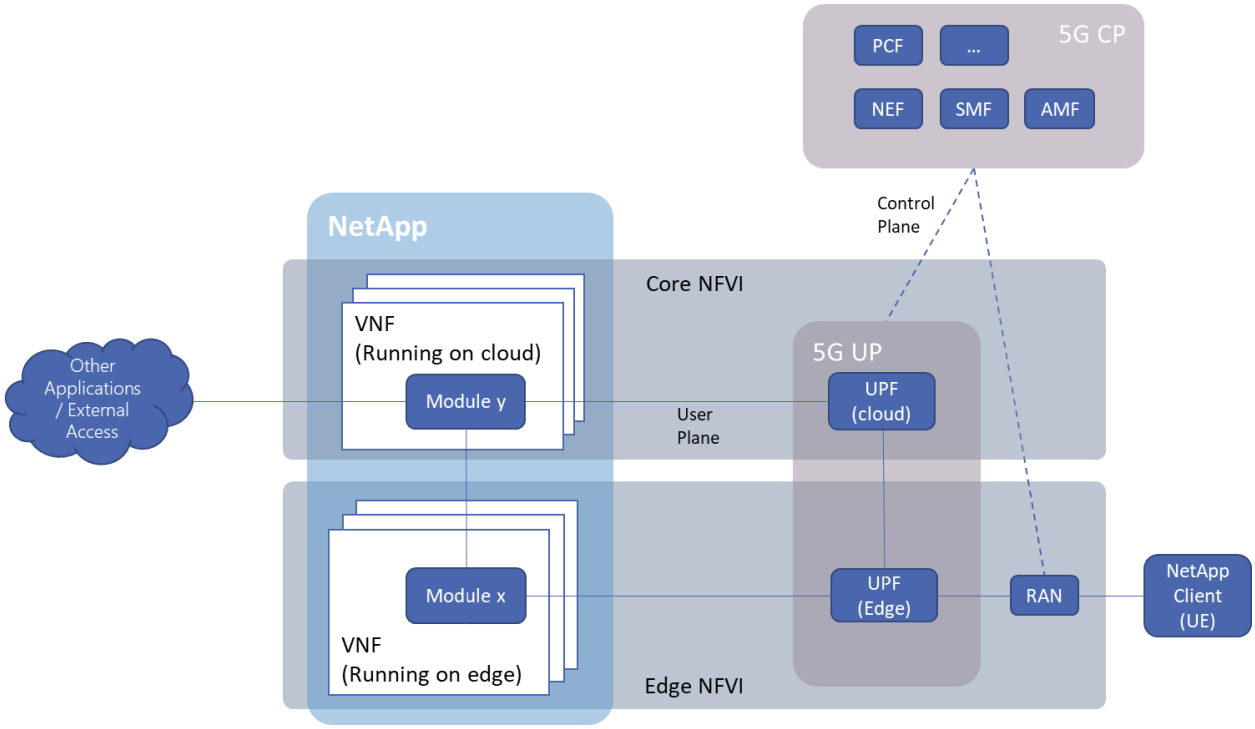

Figure 3-2 NetApp deployment over a 5G network

3.2 Smart5Grid Architecture

The goal of the Smart5Grid Platform is to provide a common place for application developers and consumers, lowering the barriers for new entrants in the energy applications market who aim at providing solutions for energy grid operators. To bring these two market entities together, Smart5Grid proposes and will develop a platform containing a repository of NetApps that have been thoroughly tested through a verification and validation framework in advance, so to be made available for consumers to use.

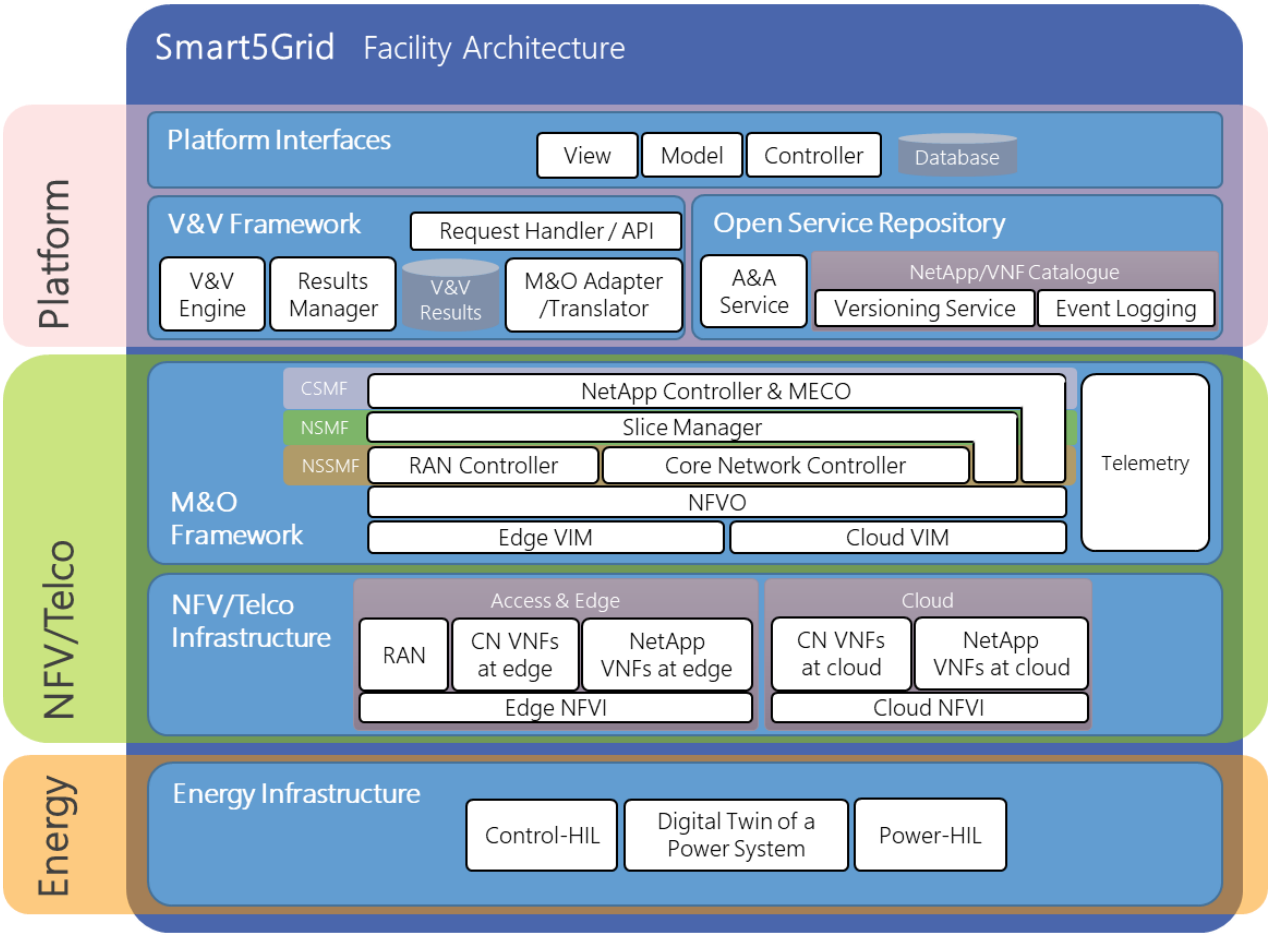

Figure 3-3 Smart5Grid functional architecture

3.2.1 Smart5Grid architecture layers

The Smart5Grid architecture is logically divided into three layers corresponding to different groups of functionalities. The first layer is the uppermost part of the architecture and contains the OSR and V&V Framework together with the platform interfaces from which users can access it. Next, we find a layer containing the virtualization and telecommunications infrastructure with its associated management and orchestration functions. And lastly, the energy infrastructure containing the grid components that connect to the NetApps services.

3.2.1.1 Platform layer

The platform layer is the uppermost part of the architecture, meaning that it is the point of entry of users to the Smart5Grid facility and where it opens for 3rd parties. This point of entry is provided by the User

Interface which, in essence, consists of a web application that manages the authorisation and authentication of users and provides access to the services offered by the exposed APIs of the other two components of this layer, namely, the OSR and the V&V framework.

The OSR is a key component of the Smart5Grid platform. This component enables developers to register their NetApps and VNFs, making them available for consumers to download and deploy over their infrastructures. Developers can also benefit from VNFs authored by other developers and combine them with their own applications forming new NetApps.

Before the NetApps and VNFs are stored in the OSR, they must undergo a testing process that provides guarantees on said NetApps to the consumers. This testing is realized by another critical component of Smart5Grid, the V&V framework. The V&V framework provides the platform with a tool that enables automated testing of NetApps in two senses: 1) Verification, which ensures that the NetApp packages and all its components and files are well formed, syntactically correct and complete; and 2) Validation, which performs tests on live instances of NetApps guaranteeing that it can perform its function with the required performance levels. The validation phase of the NetApps is supported by the NFV/Telco layer described in the next section.

More information regarding these components is provided in Section 4.

3.2.1.2 NFV / Telco layer

The execution of NetApps is supported by the NFV/Telco layer. This layer contains all the necessary elements to manage the end-to-end lifecycle of a NetApp deployment. There are two scenarios on which a NetApp deployment is considered:

1. Deployment of a NetApp by the V&V framework for validation.
2. Deployment of a NetApp by a consumer over its own infrastructure. This scenario is not facilitated by the Smart5Grid Platform and it is mentioned here for completeness. The consumer must count however, with an Infrastructure and M&O framework that offers similar functionalities as the ones described in this section, such as the lifecycle management of NetApps, to benefit from all their features.

This layer description specifies the required computing and networking systems that enable the deployment of NetApps on both scenarios, and it is subdivided in two parts that are very tightly related. These two parts are, the M&O framework, and the NFV/MEC/Telco Infrastructure itself.

The M&O framework is responsible of managing the end-to-end lifecycle of a NetApp deployment. It also provides services to cover all aspects of the complete lifecycle, including onboarding, instantiation, monitoring, scaling, and termination.

The infrastructure part of this layer is, nonetheless, as important as the M&O framework in this inseparable tandem. The infrastructure required is of two kinds primarily: computing and networking. The computing infrastructure is utilized by the M&O framework to deploy the software components in the form of containers that constitute a NetApp. This computing infrastructure can be centrally located or placed at the edge to benefit from reduced latency communications. The networking infrastructure is formed of

networking nodes in both access and core domains such as 5G gNodeBs[20] and CN functions which are orchestrated to meet the traffic demands of a NetApp.

Detailed information regarding the components of this layer is provided in Section 4.

3.2.1.3 Smart energy grid layer

At the bottom of this architecture, but not less important as it gives sense to the other layers, we find the energy infrastructure. In this layer, we find the energy infrastructure devices that this architecture is built around.

The Energy Infrastructure layer is composed of a heterogeneous set of devices from across the generation, transmission, distribution, and consumption network segments, as well as any other auxiliary devices that may be required for operating and maintaining the grid, such as cameras or sensors. These devices are the ultimate subject of the function performed by the NetApps. Through the Telco network, devices are able to reach the NFV infrastructure where the NetApp components are executed and connect to their offered services.

Furthermore, Smart5Grid integrates a Real-Time Hardware-In-the Loop (RT-HIL) testing infrastructure which enables the setup of a digital twin of a power system and integrates it with real devices. This infrastructure is pivotal in the pre-pilot testing and validation phase of the software solutions developed.

More details regarding the Energy Infrastructure layer are described in Section 4.

3.3 Smart5Grid User Roles and Scenarios

As previously introduced, the platform´s design considers two main roles (plus a third Admin role). On one side, the developers of NetApps and VNFs who want to take advantage of the platform to verify and validate their applications achieving, at the same time, visibility from consumers. Complementarily, application consumers can find applications that meet their functional and performance requirements. Based on these main roles, we can generalize and define three types of users of the Smart5Grid platform, described as follows:

- Default: A user with minimum rights who can access only the publicly available resources (NetApps/VNFs) and can also view and download their associated code.
- Developer: A user with advanced rights on the application who has all the permissions of the previous role (Default) and additionally can create, update, delete NetApps or VNFs that they own, upload code, and change the accessibility permissions, making a NetApp/VNF public or private. A Developer user that owns a NetApp can also invite other users registered in the platform and give them access to edit the NetApp/VNF code.
- Admin: A superuser allowed to perform all available actions on the resources.

Figure 3-4 shows a diagram representing these main actors and the main functionalities of the platform.

[20] Node B is the radio base station for 3G UMTS (Universal Mobile Telecommunications System), while eNodeB is the radio base station for 4G LTE (Long Term Evolution). The gNodeB is the logical 5G radio node, the equivalent of what was called NodeB in 3G-UMTS and eNodeB or eNB (i.e., evolved Node B) in 4G-LTE, is now called as the "next generation NodeB".

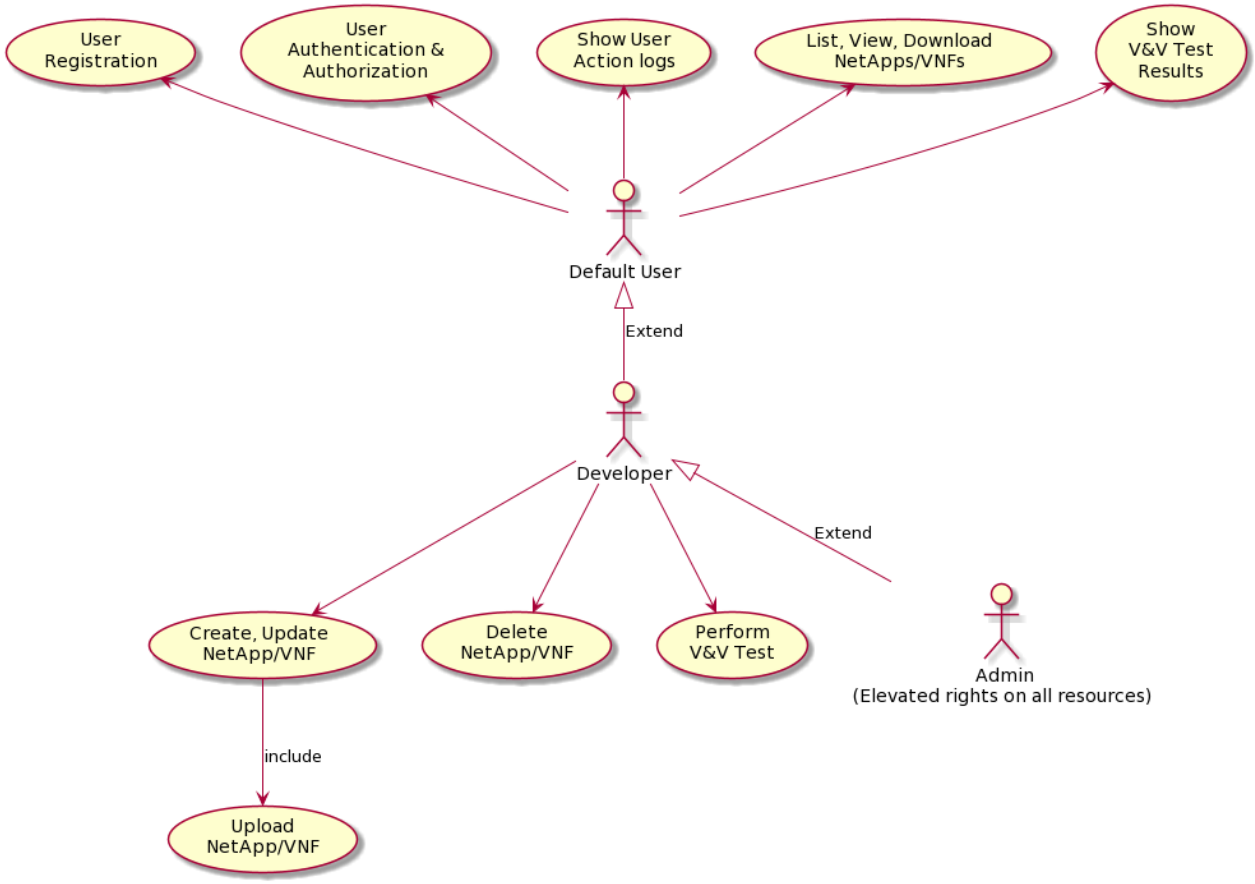

Figure 3-4 Platform Main Functionality and Actors Diagram

4 Technical specifications and technology enablers

The Smart5Grid project aims to make existing energy infrastructures safer and more resilient from an operational point of view. With this view, Smart5Grid has adopted a flexible, and versatile architectural reference design, providing an integrated infrastructure able to fulfil the full spectrum of the communications and computational needs of the energy sector. This architectural design will contribute to transforming the energy network from a closed, monolithic, and highly predictable infrastructure to an open and flexible smart network.

In a nutshell, the Smart5Grid core functional decomposition created from the different UCs is based on the concept of NetApps, whose main purpose is to hide the complexity of the 5G telco network to the energy application developers so that they can develop an application not having to deal with the underlying network. Every unit that composes the NetApp is hosted by a VIM, such as OpenStack [17] or Kubernetes [62]. The chosen VIM provides monitoring information to the NFV MANO framework (e.g.: OSM), which in turn broadcasts information to the NetApp Controller that may employ analysis techniques to propose the optimal VNF and NetApp placing. All these functionalities are provided reserving resources through the use of a Slice Manager (SM). Another aspect tackled by Smart5Grid, that is reflected in the architecture and in the consequent specifications, is the reduction of the time-to-market for networked services and the NetApp creation, so to lower the entry barrier to third party developers of VNFs and NetApps. This is reflected in the creation of an integrated DevOps methodology that in Smart5Grid assumes the shape of the V&V framework of NetApps and NSs (VNF graphs) so that operators can be sure of their behaviour.

In the following sections, the definition of the fundamental principles, and technological choices as well as the architectural concepts and implementation scenarios will be illustrated, with the main aim to define the reference architecture supporting Smart5Grid major components synergic work.

4.1 User Interface

The User Interface (UI) facilitates user interaction with the OSR and the V&V platforms. It helps users to access and manage the NetApps and the VNFs included in them in a descriptive and well understandable manner. Also, it is the gateway for the user to initiate tests using the V&V Framework and view the results.

4.1.1 Architecture

The architecture of the web UI follows the Model – View – Controller paradigm:

- The Model handles the representation of the data in a sensible format.
- The View displays the information of the Model to the user and provides him/her the ability to perform actions.
- Finally, the Controller manages how incoming data can be mapped to Model objects, interprets actions performed in the View into actions on Model objects and updates the View when data is changed.

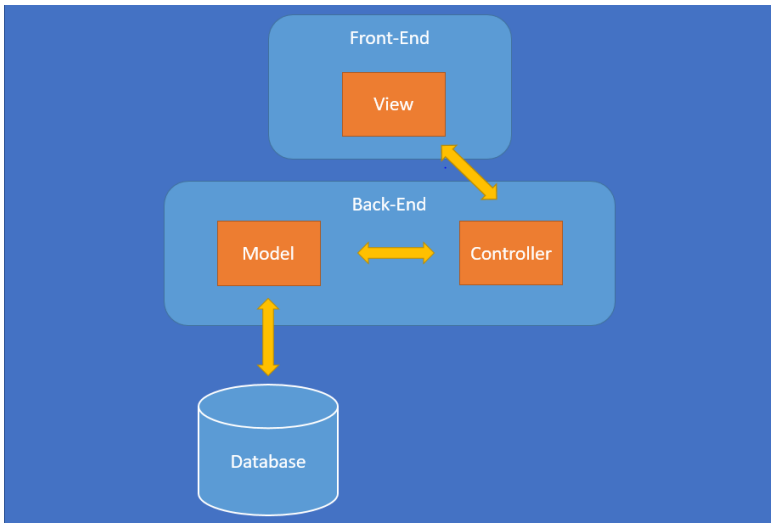

Figure 4-1 UI architecture

In our case, the View is the front-end part of the web application which communicates through Representational State Transfer (REST) API calls with the back-end server, acting as the Controller. The Model consists of the code in the back-end that implements the objects defined in the application. The Controller can interact with the Instances of the objects and such instances can be stored in the database.

4.1.2 Functional description

The User Interface acts as the main gateway for the user to interact with the OSR and the V&V platforms. Access to the UI's different functionalities is determined by a role-based access model. Roles are assigned to a user for a specific resource. The roles are defined in Section 3.3 and consist of "Default", "Developer", and "Admin". Below is a list of the available actions a user will be able to perform using the User Interface:

- User Registration: The user can register to the User Interface web application in order to request access to the available functionality.
- User Authentication and Authorization (A&A): The user, by entering the required credentials, can login to the User Interface and gain access to the application resources. The users are assigned roles. The main roles are described in the OSR section.
- List, View, Create, Update, and Delete operations on NetApp/VNF (OSR): The users, according to their access level, are able to perform the actions: List, View, Create, Update, and Delete on the NetApps and VNFs. The User Interface provides a page to list all the NetApps and another to list all the VNFs; clicking on the desired item, the user is redirected to a NetApp/VNF specific view page. By accessing the view page of a NetApp/VNF, the User Interface auto-generates a page specific to the selected NetApp/VNF showing all the information that describes it and presents to the user the actions that can be performed on it (Update/Delete). Creating a new NetApp/VNF requires the user to fill a form containing basic information. Code upload is performed after the NetApp/VNF entity is created. The view page also displays to the user the code structure of the NetApp/VNF and allows viewing the contents of the uploaded files.
- Upload/Download NetApp/VNF (OSR): Additionally, to the aforementioned actions, the user can upload and download files of the NetApp and VNF code. By visiting the NetApp/VNF specific page, user with access can download the code. Uploading code requires elevated authorization, as a developer user role, and being the owner or being invited to access the NetApp/VNF.

- Perform V&V test (V&V): The User Interface also facilitates triggering the V&V tests of existing NetApps. This action also requires the developer user's role. After the test is requested, it goes to pending state, upon the reload of the page the User Interface requests the latest test status. A NetApp/VNF cannot become publicly available if the V&V tests are not successfully completed. Further changes on the code require performing the V&V tests again.
- Show V&V test results (V&V): The V&V platform stores the history of all performed V&V tests. The User Interface can request the test results per NetApp/VNF.
- Show User action logs: Actions performed on the NetApp/VNF entities of the OSR are stored on the OSR Service. The User Interface can request and display such logs to the NetApp/VNF specific page.

4.1.3 Technical specifications

As mentioned earlier, the UI comprises of three main components, that is the front-end, the back-end and the database. The database storing the user information will be shared with the OSR platform implementation of the A&A Service. Hence, the User Interface and the OSR mainly address the same groups of users, that is developers of NetApps or VNFs and external users with interest in the NetApps and VNFs. Therefore, the implementation of user management on both services can be fulfilled by an interoperable A&A service.

The front-end or the "View" of the application should be a modern web framework that facilitates the creation of a dynamic application with the minimum possible code complexity. It should offer fast page rendering and a responsive UI that can be displayed on both desktop and mobile devices.

The back-end will implement both the Controller and the Model definitions of our chosen architecture. It exposes REST interfaces to the front-end and translates user actions on the UI to requests towards the appropriate external component. It gathers the data returned by external applications, creates instances of the defined objects, and exposes them to the front-end.

4.1.4 Interfaces and data to be exchanged

The User Interface requires specific interfaces from the OSR and the V&V platforms. The interactions taking place for the available operations on the User Interface are being explained in the diagrams below.

User Login

Before every interaction with the User Interface, the user must login. After the user logs in, using the OSR's A&A service, the user's browser receives an authentication token that contains in its payload the user role referring either on the application or on specific resources. For example, users with the admin and developer roles on the application level will be able to create a new NetApp or VNF (considering the User Interface application to be the resource on which the role applies in this case).

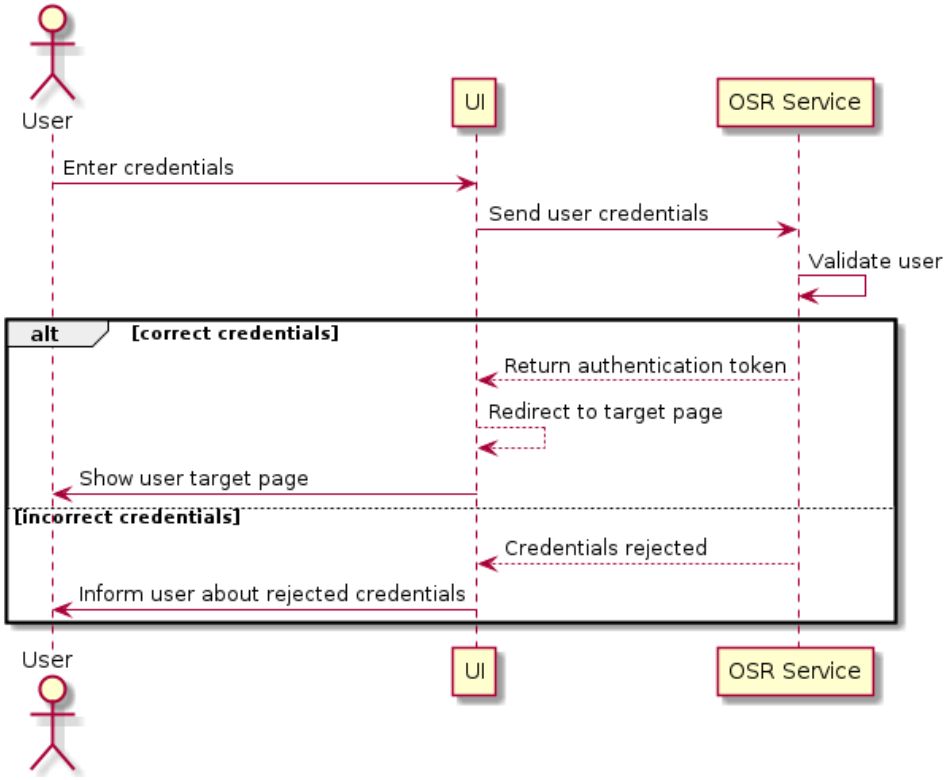

Figure 4-2 User Login

Create NetApp / VNF

The user logs in and the OSR service returns the user role on the application level in the access token. Having the right user role will determine if the "Create NetApp (or VNF)" button will be shown to the user. By clicking on the button, a modal window appears where the user can fill the NetApp/VNF information. Then, the information is sent to the OSR service where a check is performed on whether the NetApp/VNF name is unique. If it is not unique, the user is informed to try a different name, otherwise the NetApp gets created in the OSR. Then the user browser shows a success message and redirects to the newly created NetApp/VNF specific page.

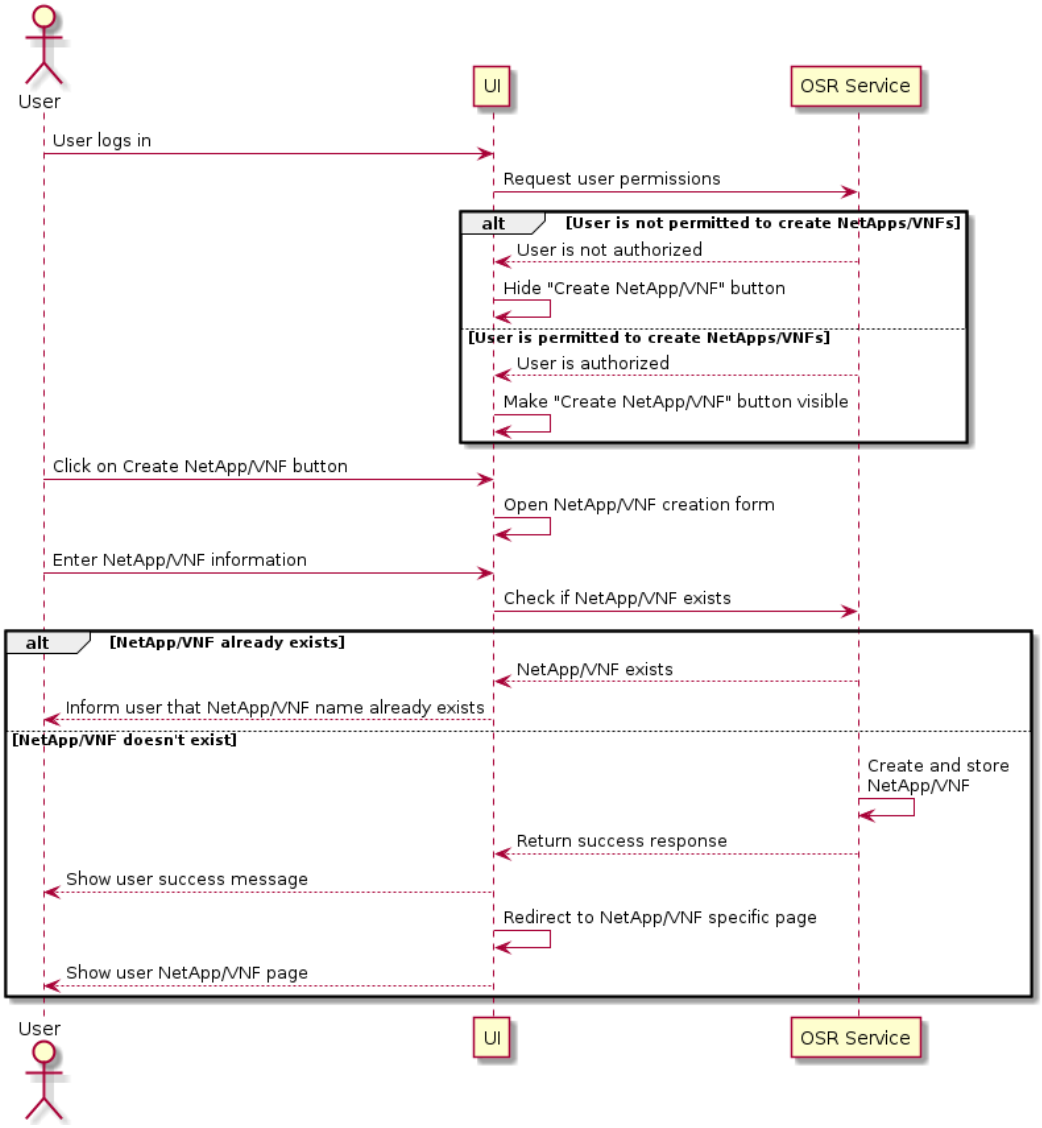

Figure 4-3 Create NetApp/VNF

List NetApp / VNF

The user, considered logged in, clicks on the "List NetApps/VNFs" tab. The list information is retrieved from the OSR service and displayed to the user.

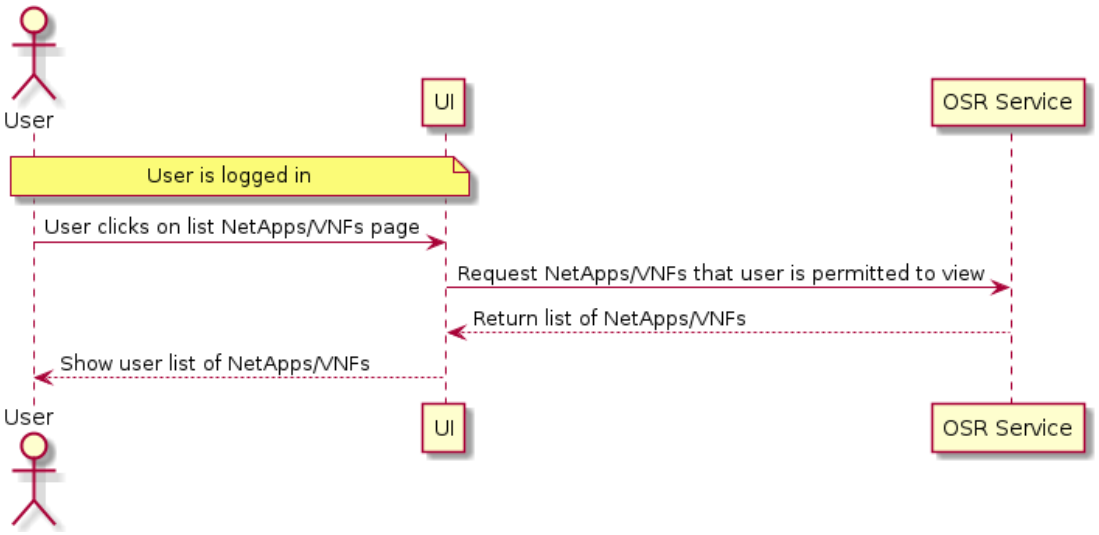

Figure 4-4 List NetApp/VNF

View specific NetApp / VNF

The user is considered logged in and he/she can view a list of NetApps/VNFs. He/she clicks on a NetApp/VNF hyperlink text and is redirected to a NetApp/VNF specific page. The information is retrieved from the OSR service and displayed to the user.

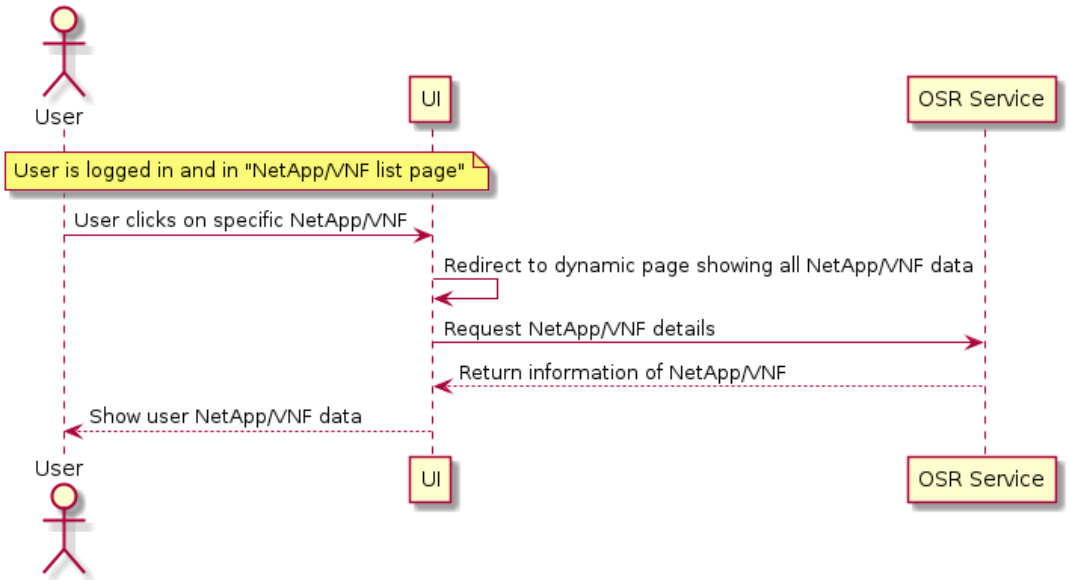

Figure 4-5 View specific NetApp/VNF

Update NetApp / VNF

The user is considered logged in and he/she can view a list of NetApps/VNFs. He/she clicks on a NetApp/VNF hyperlink text and is redirected to a NetApp/VNF specific page. The information is retrieved from the OSR service and displayed to the user. Also, the user role on the NetApp/VNF is retrieved. If the

user has the needed permissions, the "Update NetApp/VNF" button will be displayed. By clicking it, a modal window appears where the NetApp/VNF info can be edited. Submitting the changes, after confirmation, the new information is sent and saved at the OSR service. After that, the page is reloaded with the updated data.

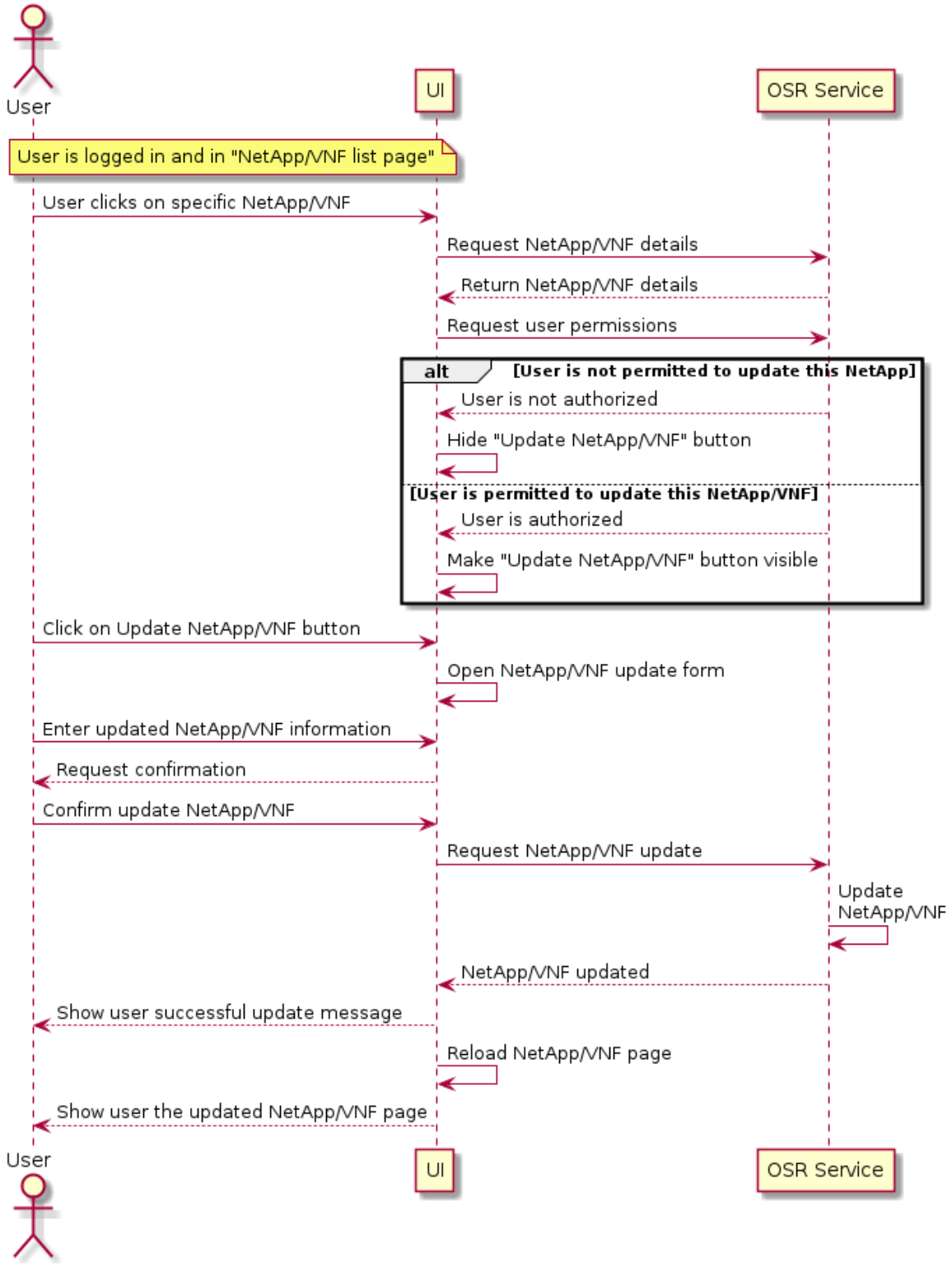

Figure 4-6 Update NetApp/VNF

Delete NetApp / VNF

Same as above, if the user has enough permissions, a "Delete NetApp/VNF" button becomes available, this time causing the NetApp/VNF to be deleted in the OSR service.

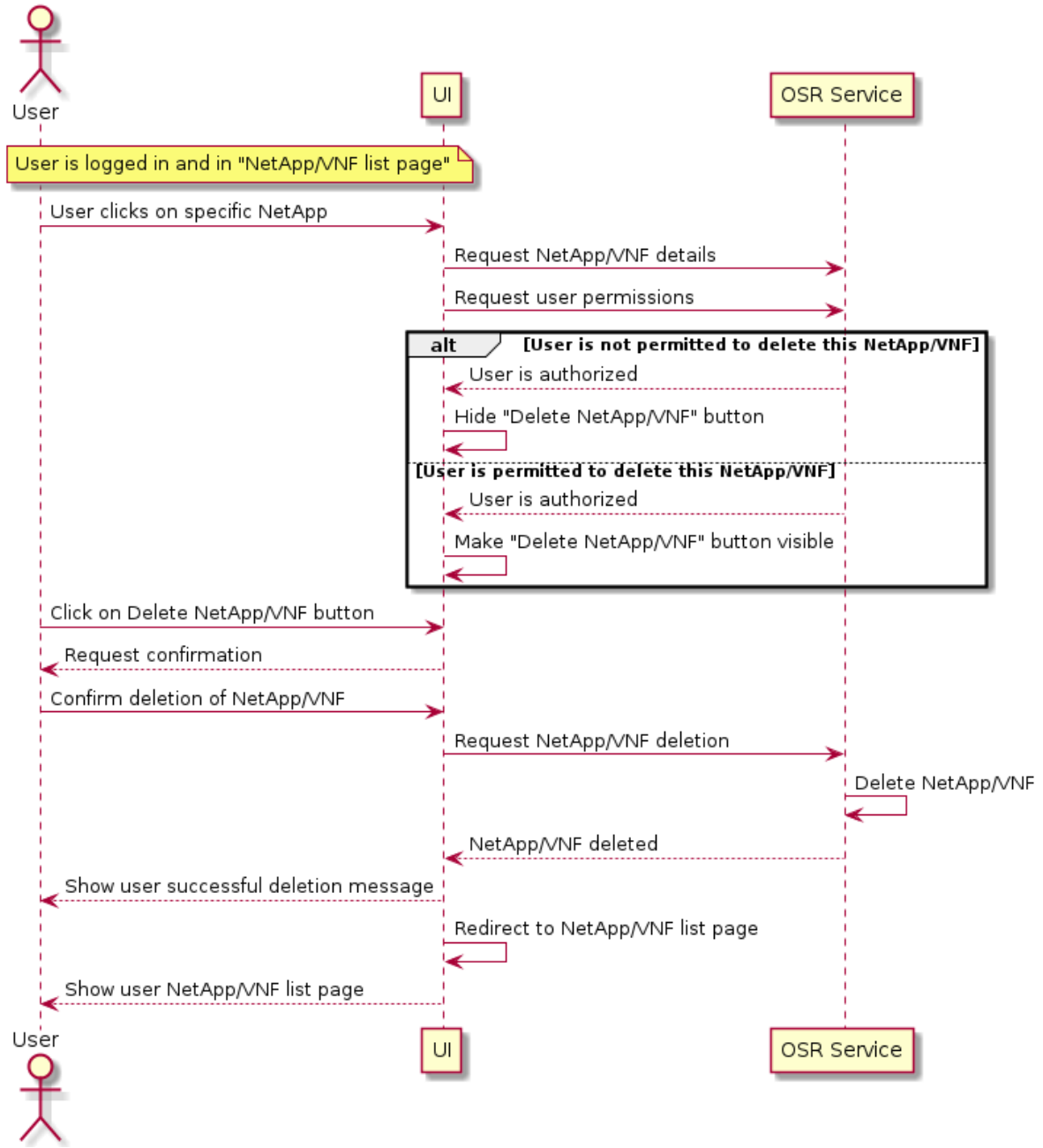

Figure 4-7 Delete NetApp/VNF

Upload NetApp / VNF

Uploading a NetApp/VNF workflow is similar to the previous ones. The "Upload NetApp/VNF" button brings up a modal window that gives the user the ability to browse files on their local device to choose which ones to upload in the OSR service.

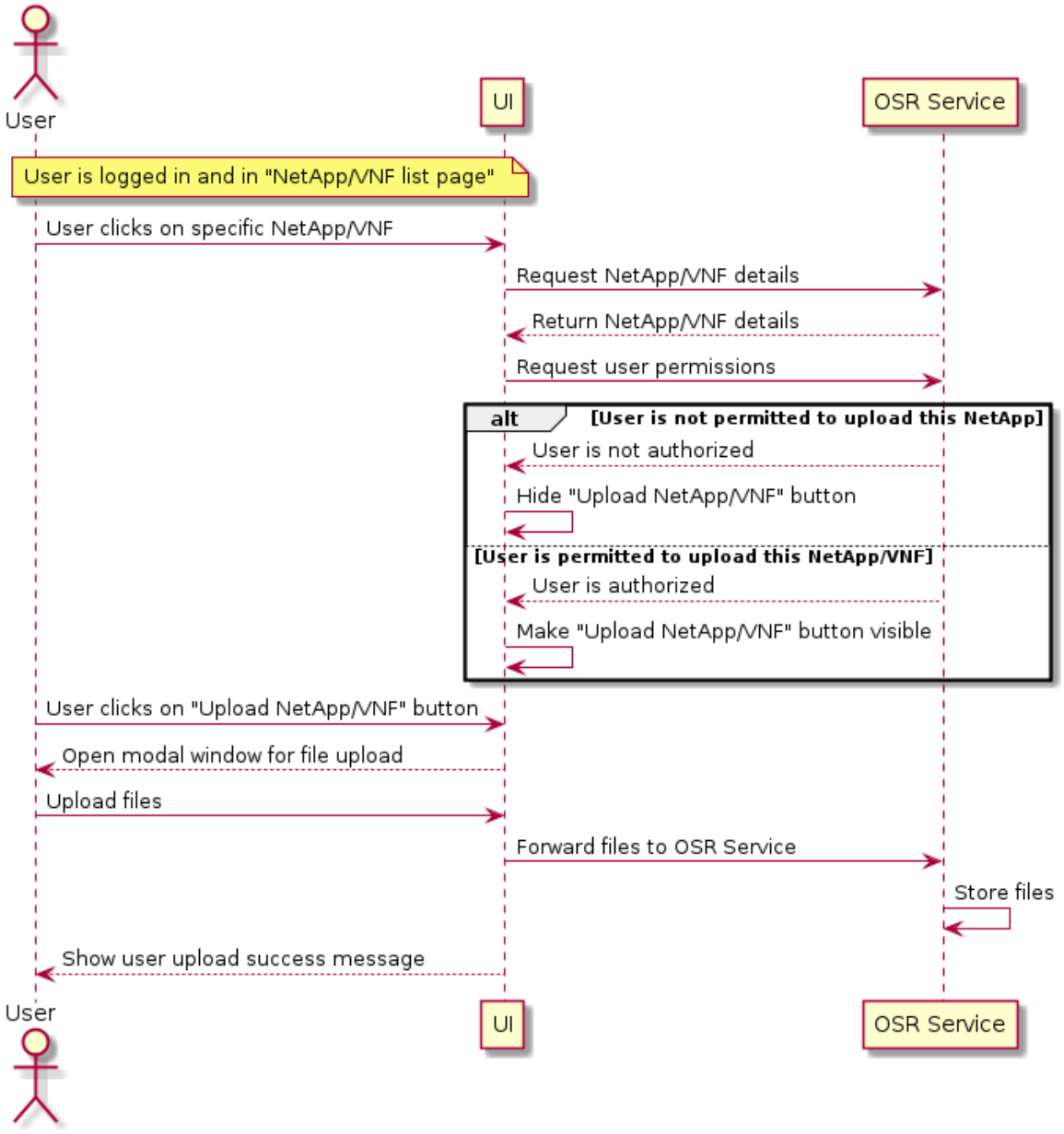

Figure 4-8 Upload NetApp/VNF

Download NetApp / VNF

In the case of NetApp/VNF download, if a user has access to view the NetApp/VNF, then he/she can also download it. Clicking on the "Download NetApp/VNF" button will cause the OSR service to generate a compressed file of the source code of the NetApp/VNF and the UI will redirect to the OSR link that makes the compressed file available for download to the user.

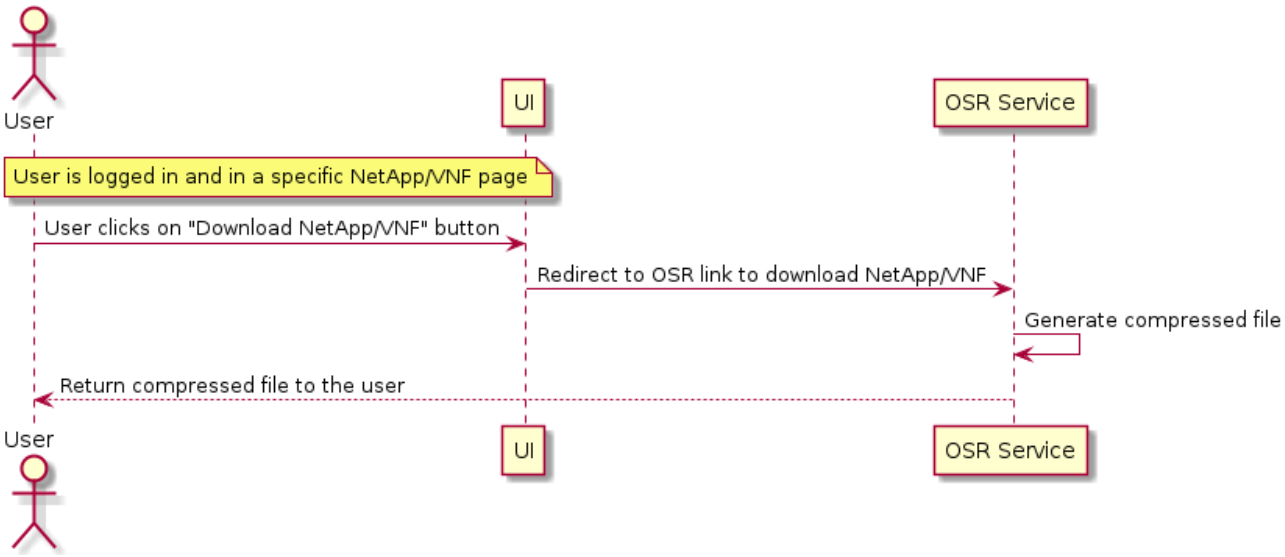

Figure 4-9 Download NetApp/VNF

Show user event logs

A page with all the event logs of the application will be available only to the users with user role admin on the application level. The user role in the authentication token returned from the OSR determines if the tab will be visible or not. When requested, the data are retrieved from the OSR service and presented to the user in the UI.

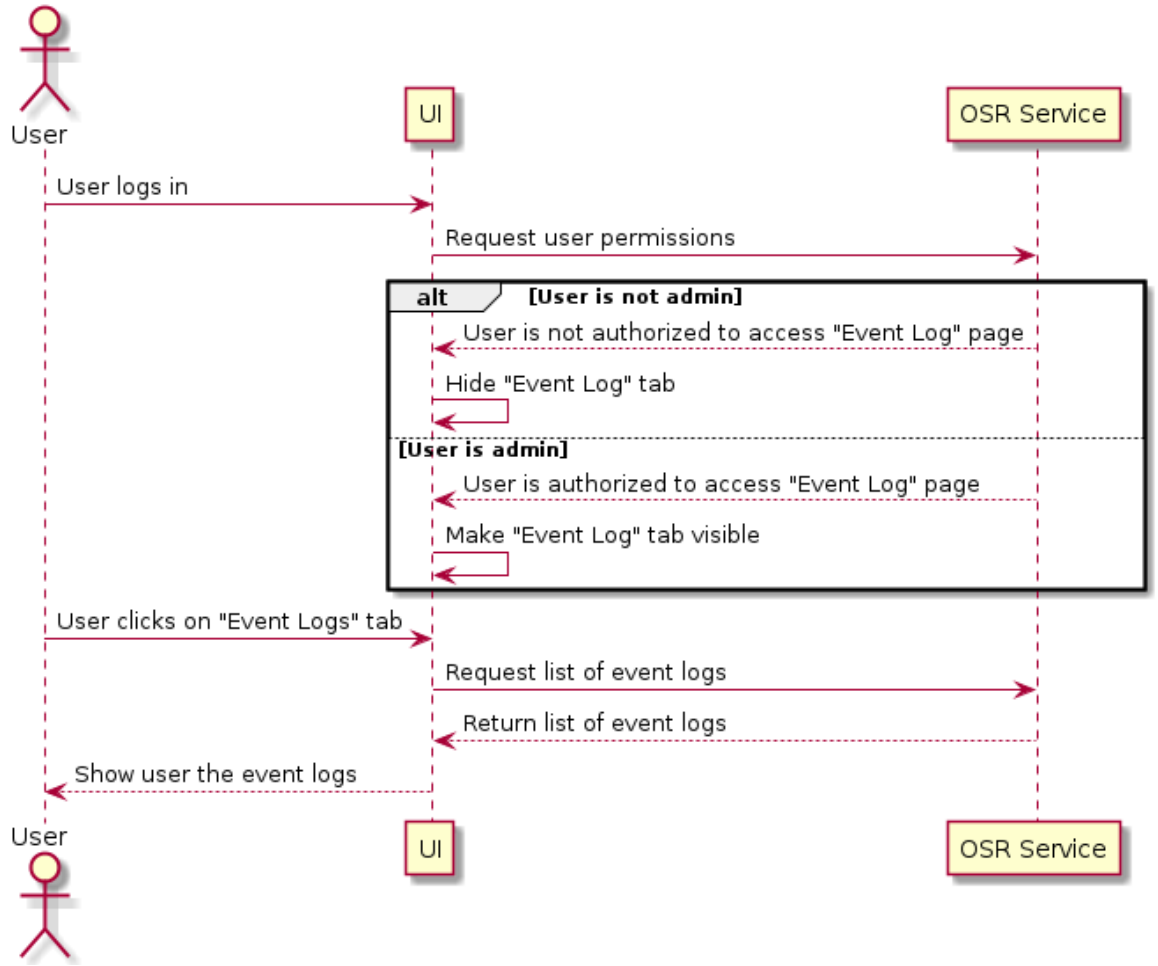

Figure 4-10 Show user event logs

Launch V&V test

To perform a test on a NetApp using the V&V platform, the user must first login in the UI via the OSR service. If the required permissions exist, the UI forwards the request to the V&V platform and returns the successful feedback to the user browser. This action does not return the result of the test as the test in the V&V platform may require significant time to complete,

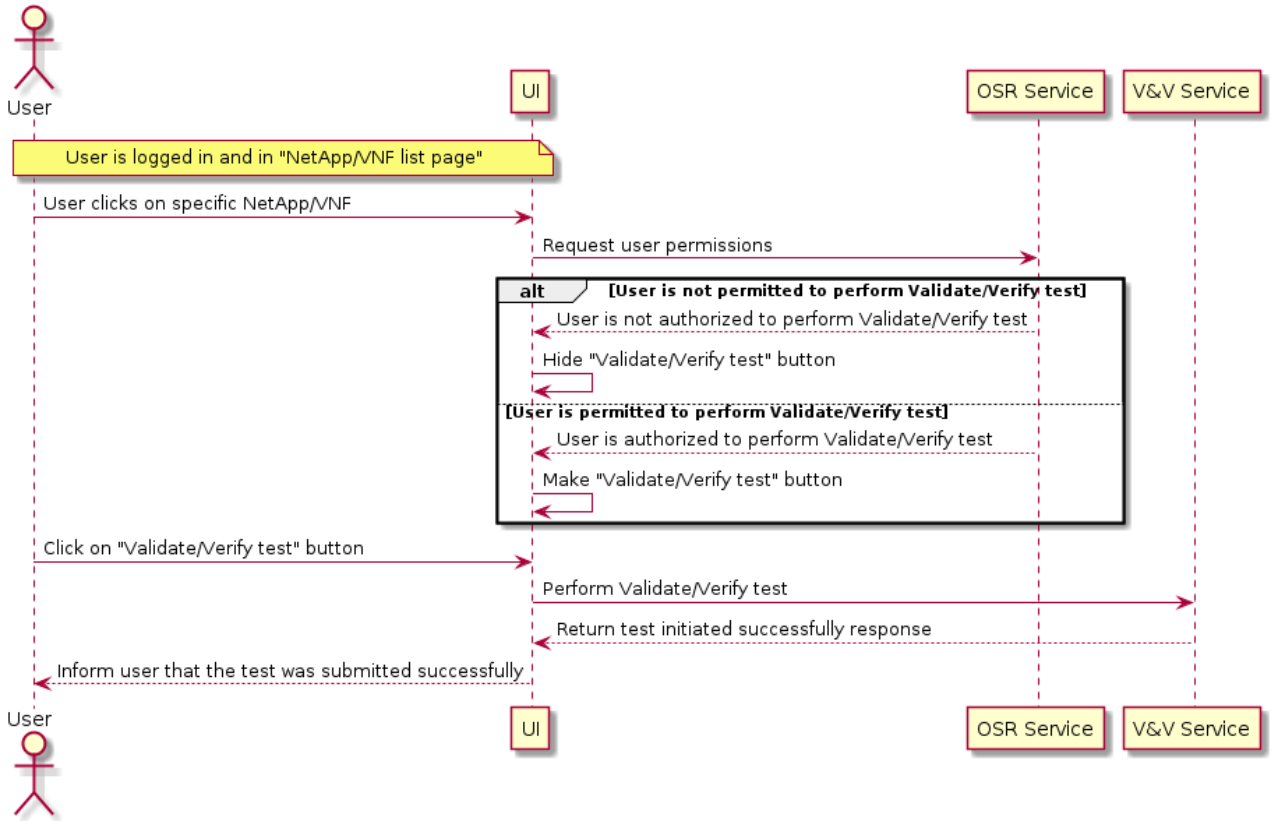

Figure 4-11 Launch V&V test

Get V&V test results

The user is considered logged in and, on a NetApp/VNF specific page. To get the results of the latest V&V test, the user clicks on the "Validate/Verify test results" button, the UI sends a request to the V&V platform, where the results are stored, receives a response, and displays the results to the user.

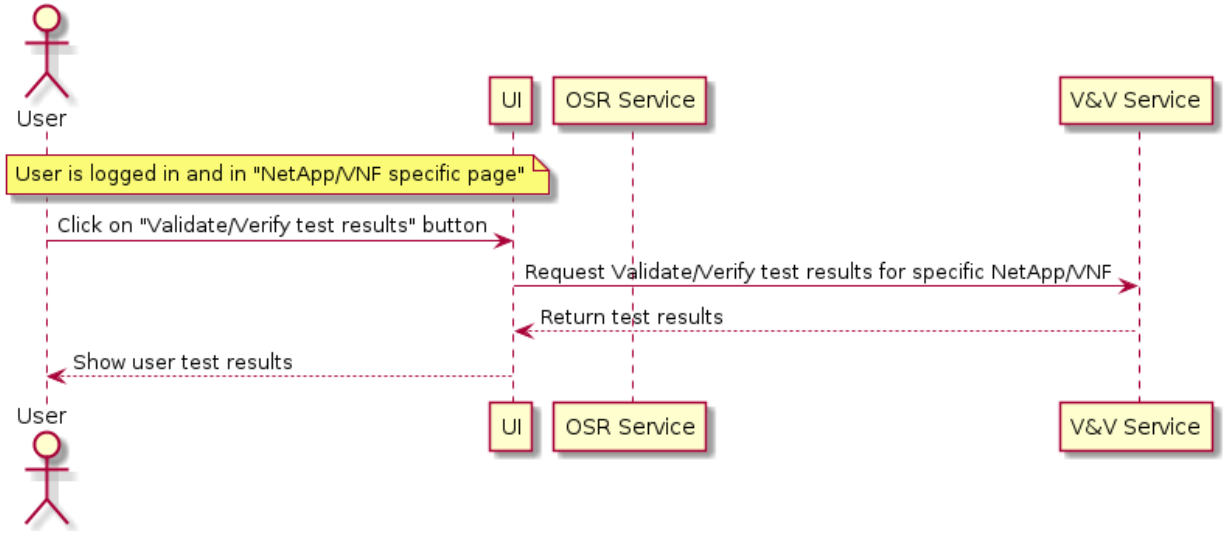

Figure 4-12 Get V&V test result

4.1.5 Security

As the User Interface is a publicly available service, users need to be able to trust the web application. The code they upload is their intellectual property and must be protected by malicious and/or unauthorized users. The service uses the Hypertext Transfer Protocol Secure (HTTPS) protocol[21] providing Transport Layer Security (TLS) encryption to all requests.

4.2 Open Service Repository

The OSR is the service responsible for storage and management of all the NetApps and their included VNFs. It provides secure connection to authorized users, a code repository for the code of the applications, tracking of all changes and log reporting to the users. The available functionality will be exposed to external components through REST APIs.

4.2.1 Architecture

The OSR consists of the A&A service and the NetApp/VNF Catalogue. The latter includes a Code Versioning service and an Event Logging component.

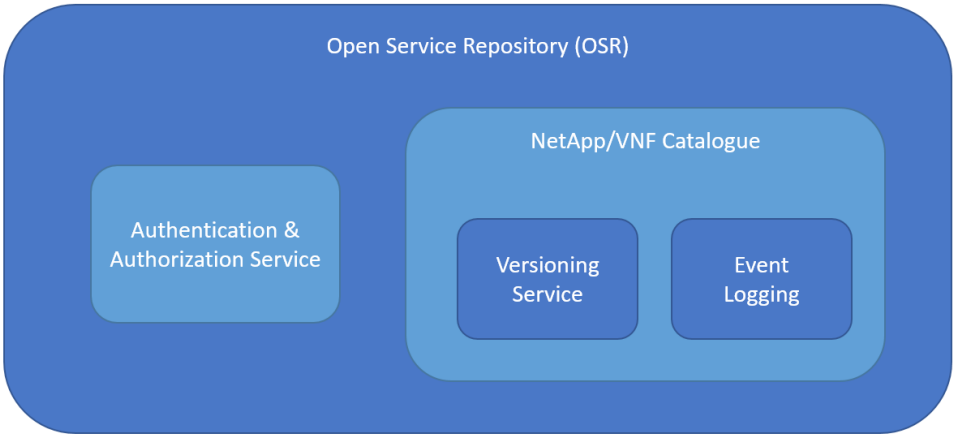

Figure 4-13 OSR functional Architecture

- A&A Service: This service is responsible for user authentication and role-based authorization on the operations provided by each OSR component.
- NetApp/VNF Catalogue: It stores and links all NetApp and VNF information. NetApps and VNFs are stored in the Code Versioning Service and logs are stored in Event Logging component. The Catalogue component acts as the interface of the aforementioned components to external actors. It also has its own database to store NetApp and VNF data. Access to the instances of the NetApp/VNF Catalogue objects is realized through the A&A Service.

[21] The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser. Hypertext Transfer Protocol Secure (HTTPS) is an extension of the HTTP. It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS or HTTP over SSL. For further details also see; https://en.wikipedia.org/wiki/HTTPS.

- Code Versioning Service: It is the backend service required to store the code and track changes, based on existing GIT (Global Information Tracker) implementation.
- Event Logging: It keeps records of all events that occurred by the users. Actions taking place at the NetApp/VNF Catalogue and the Code Versioning Service are being logged by the Event Logging component. To collect the logs from every component, agents will be installed alongside each component.

4.2.2 Functional description

OSR A&A Service manages users and user roles. User information such as the user login credentials are stored in the "user" objects. User roles represent the user level of authorization over specific resources in the OSR service. The roles are mapped to users and OSR resources (e.g.: NetApps, VNFs) to access different features of the other OSR components. The main user roles are "default", "developer", "admin" as described in Section 3.3.

The NetApp/VNF Catalogue is the main component of the OSR service. The main feature it offers is storing the NetApps and the VNFs. It allows users to perform CRUD (Create, Read, Update, Delete) operations on the NetApps and VNFs as well as upload and download files. It communicates with the A&A service to decide whether a user can access a resource or not.

The files contained in the NetApps and the VNFs are stored in the Code Versioning service and the OSR Catalogue makes the necessary calls to it to forward the files during the upload and download operations while persisting the mapping between NetApp and its files on the Catalogue database. Also, during all the operations, the Catalogue is responsible to push the log information to the Event Logging service. This takes place after the operation is successfully completed and before returning the result to the user or external component that initiated the request.

The Code Versioning Service acts as the backend of OSR Catalogue for storing files of NetApps and VNFs. It permits the users to work simultaneously on the same project, without interfering with other users' work. Branching allows users to work on a line that runs parallel to the main project files. It is compatible with all major OSs. It keeps a record of all the commits done by each of the collaborators. A log file is maintained and is pushed to the central repository each time the push operation is performed. So, if a problem arises, it can be easily tracked and handled by the developer. The data are being stored in a relational database. Apart from the APIs made available through the OSR Catalogue (upload/download operations), the user will be able to circumvent this process and directly use the Code Versioning service providing common git functionality. Event logs of such user actions will be recorded to Event Logging component using an agent service as explained below.

The Event Logging component is responsible for storing all the logs gathered from actions performed on OSR objects, such as NetApps, VNFs, code repositories, files, etc. The data are being gathered either by pushing the data to the server or using agent services. Pushing the data to the server is done by simple HTTP requests. The agents, when applied, can monitor the specified log files or location, collect log events, and forward them to the Event Logging component in a unified format. Apart from storing the log data, the Logging component offers the communicating components the ability to query the desired data logs applying time or object properties filters.

4.2.3 Technical specifications

A&A Service will be an implementation of a software system that stores, organizes, and provides access to information. The objects stored in it will be the users, the user roles, and the resources that the users can act upon. The role-based access requirement will be fulfilled by linking user instances to resources and assigning a user role to them. Such requirements can be met by a relational database or an active directory service and an overlay software solution. Both existing open-source solutions and a new custom one will be assessed. A&A Service will need to be integrated mainly to the OSR Catalogue component, but it would also be desirable to be compatible with the Code Versioning Service, in the case that direct access is needed for users. Consequently, the solution given should provide the interoperability needed, the user should be able to log in with a single ID and password to both, independent, software systems.

The NetApp/VNF Catalogue will be a custom software application, a back-end application that will provide the necessary REST APIs for other systems to communicate with. A database will be needed to store NetApp and VNF information as well as the data linked to them such as the files at the Code Versioning Service and logs at the Event Logging component.

The Code Versioning Service will store the NetApp and VNF code and be able to track the changes applied to the files of the code. Also, it allows multiple developers to work together on and support non-linear development through parallel code branches. It will be based on an existing open-source implementation of GIT. Additional required features will be developed either as add-ons or an overlay application.

The Event Logging Component will be receiving log data from different sources. The data need, eventually, to be in a unified format. Data coming from the NetApp/VNF Catalogue will be easy to manipulate before being sent to the Event Logger. On the other hand, data stored in other components will need to be retrieved with the help of agents that will read and single out the required log records and then transform and send them to the Event Logging component. Existing open-source data collectors can be used for the part of agent-based log collection. The overall unification, querying and presentation of the data will be implemented as a custom software application exposing REST APIs.

4.2.4 Interfaces and data to be exchanged

The interfaces provided by the OSR are explained in the sequence diagrams that follow. "User" or "External Component" are the parties that can communicate with the OSR using its REST APIs. The sequence diagrams whose title overlaps with those in the User Interface section, explain the internal communication of the OSR components.

User Authentication

To become authenticated, the user must send the credentials to the OSR A&A service. If the credentials are validated, the OSR A&A will return an authentication token otherwise an error message.

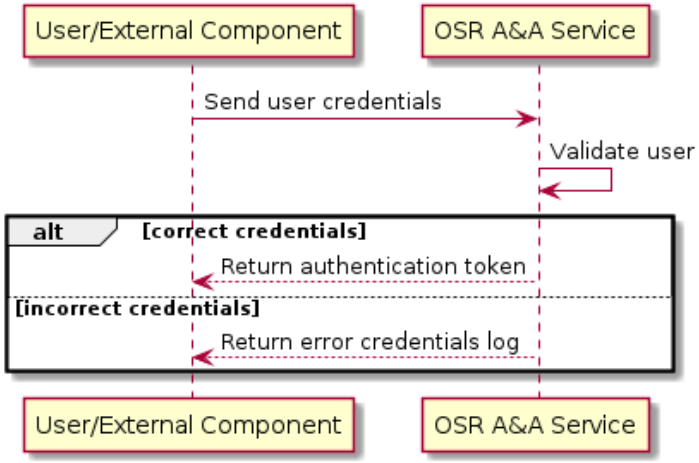

Figure 4-14 OSR User Authentication

Create User

In order to create a new user, the user that initiates the request must be authenticated and also have the required permissions for the action. The user information sent with the request are then stored to the OSR A&A and the new user is created.

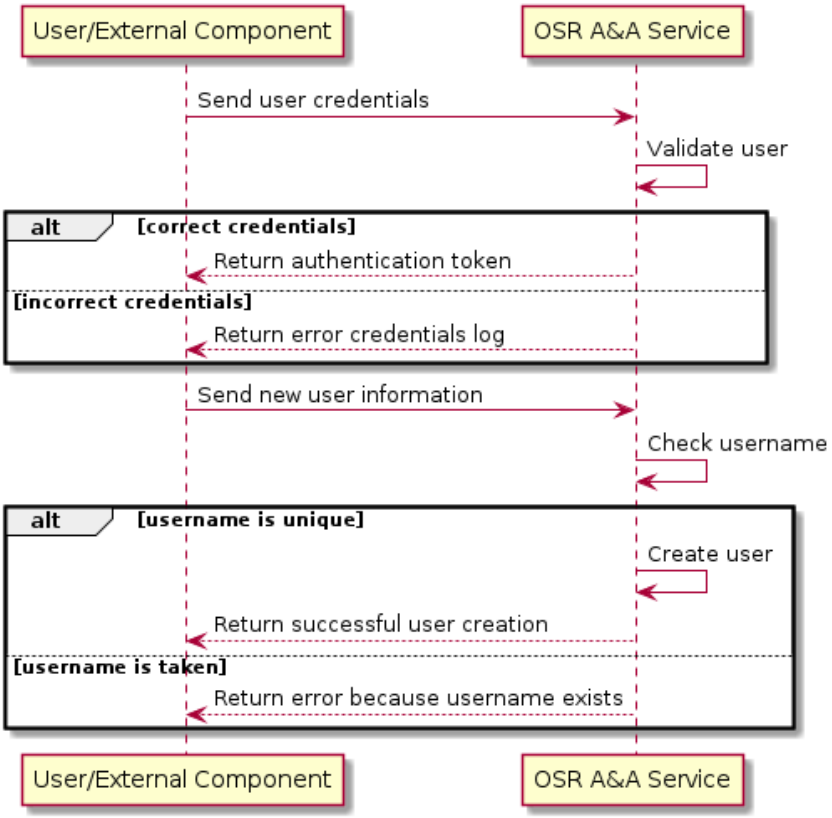

Figure 4-15 OSR Create User

List Users

A request with the required permissions can return a list of the users.

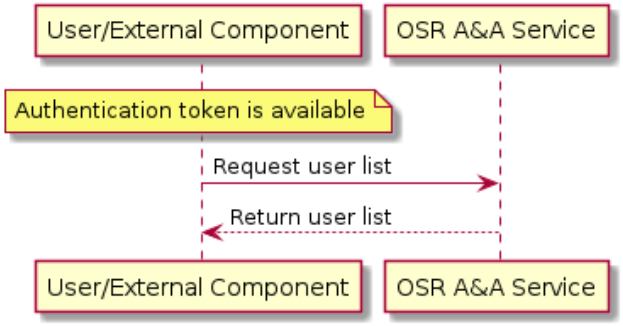

Figure 4-16 OSR List Users

Show User

A request to show the details of a specific user. The id or username must be provided in the request payload.

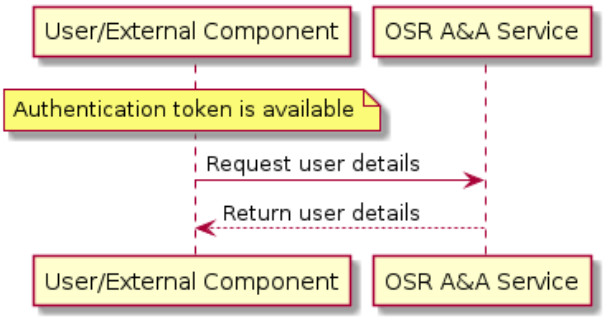

Figure 4-17 OSR Show User

Update User

A request to update the details of a specific user.

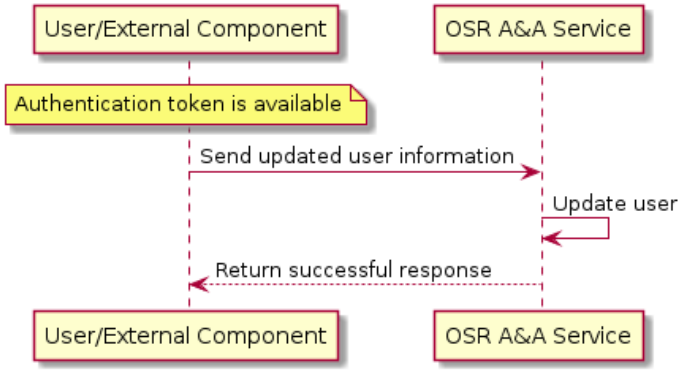

Figure 4-18 OSR Update User

Delete User

A request to delete a specific user.

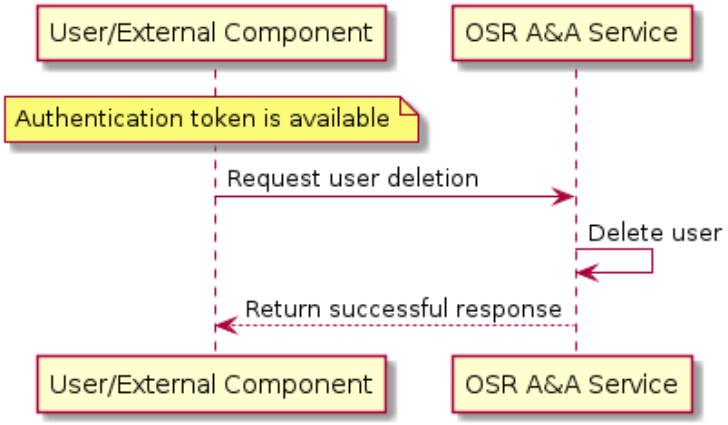

Figure 4-19 OSR Delete User

Create NetApp / VNF

The request to create a new NetApp or VNF requires the following interactions between the OSR components: The user sends the NetApp/VNF information to the Catalogue service. If the user has the required permissions, the request proceeds. The Catalogue performs a check to verify that the NetApp/VNF has a unique name. If so, the Catalogue communicates with the Code Versioning service to create a corresponding project. After the project is created, the Catalogue sends the log of the action to the Event Logging component.

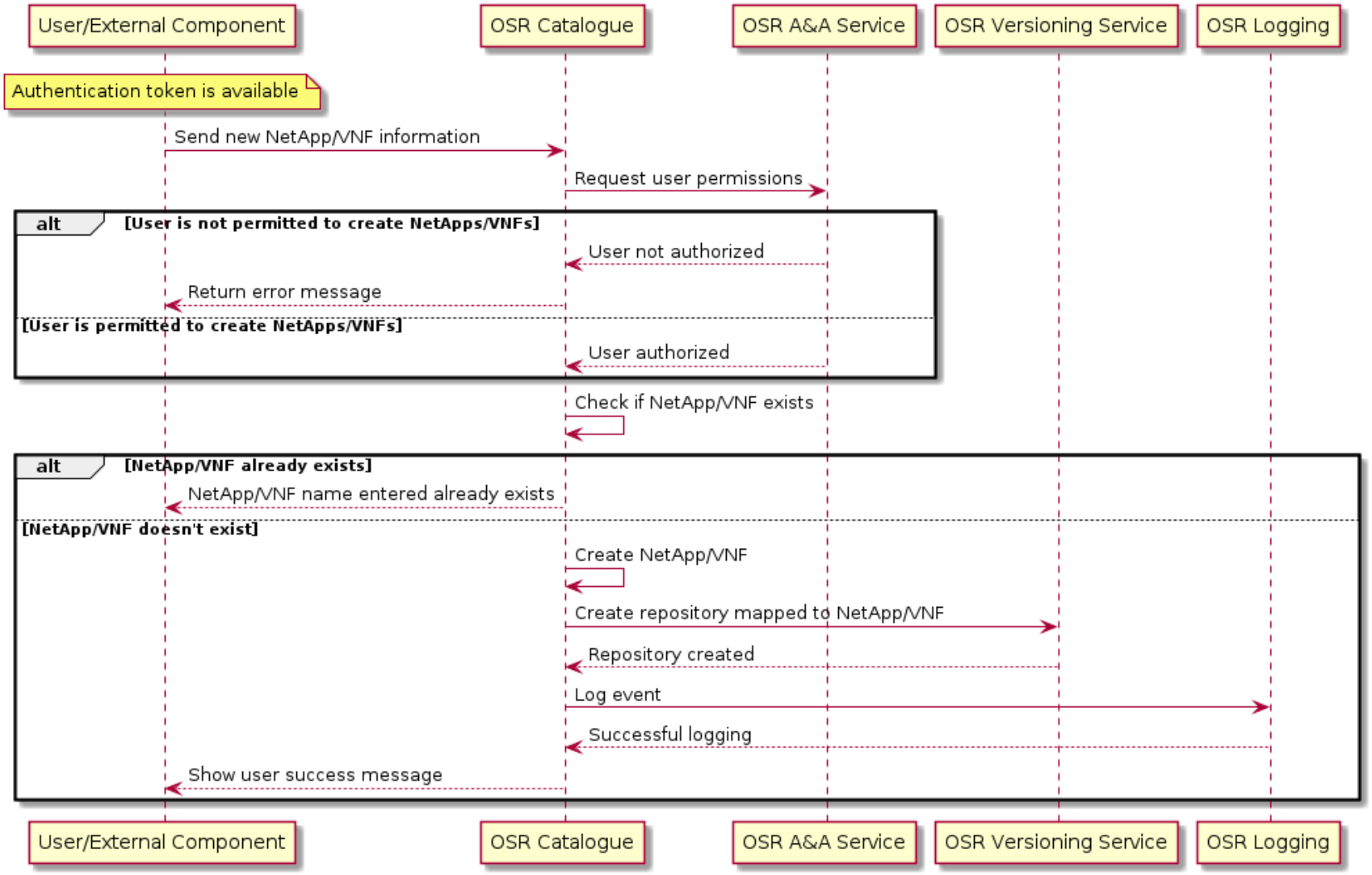

Figure 4-20 OSR Create NetApp/VNF

List NetApps / VNFs

The request towards the Catalogue to list NetApps/VNFs requires authorization from the A&A service. The user can get the NetApps/VNFs that he/she owns or that are publicly available.

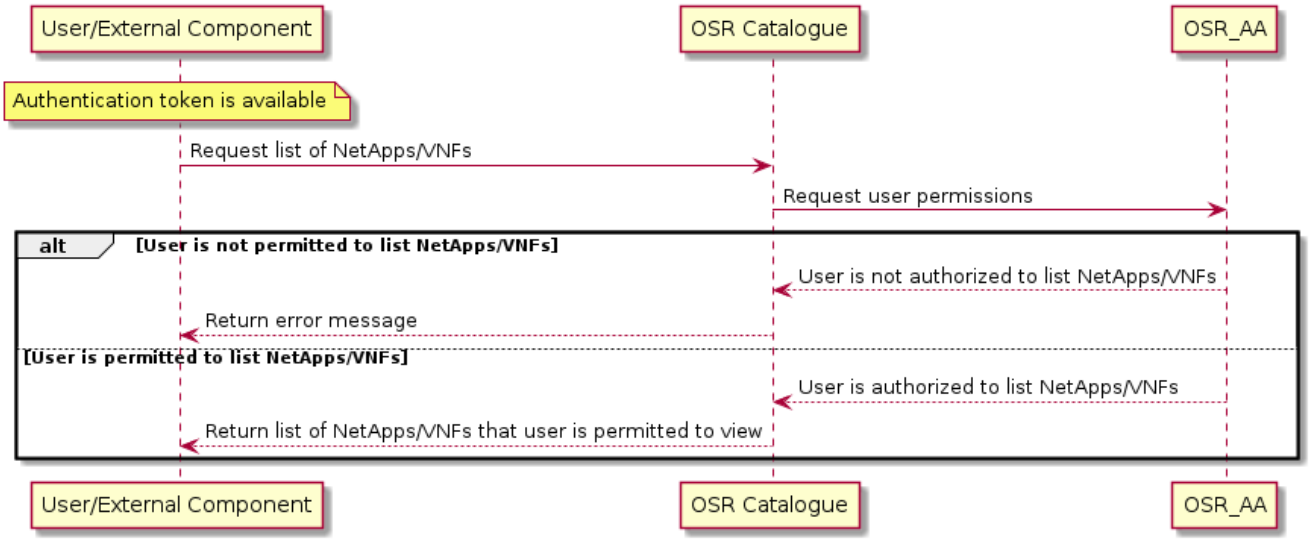

Figure 4-21 OSR List NetApps/VNFs

Show NetApp / VNF

The same as with the "list" action, getting the details of a specific NetApp/VNF requires the user to be authorized to access the specific NetApp/VNF.

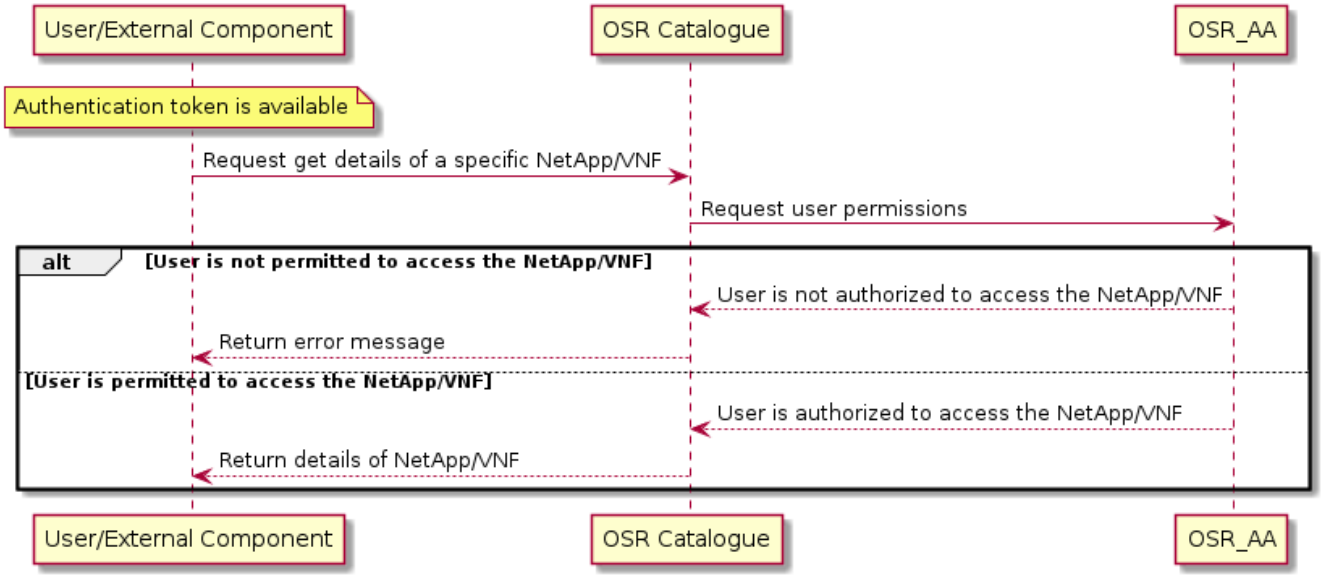

Figure 4-22 OSR Show NetApp/VNF

Update NetApp / VNF

To update the NetApp/VNF, the user sends the updated info in the request payload towards the Catalogue service. The NetApp/VNF project must then be also updated in the Code Versioning service. The action is logged to the Event Logging component.

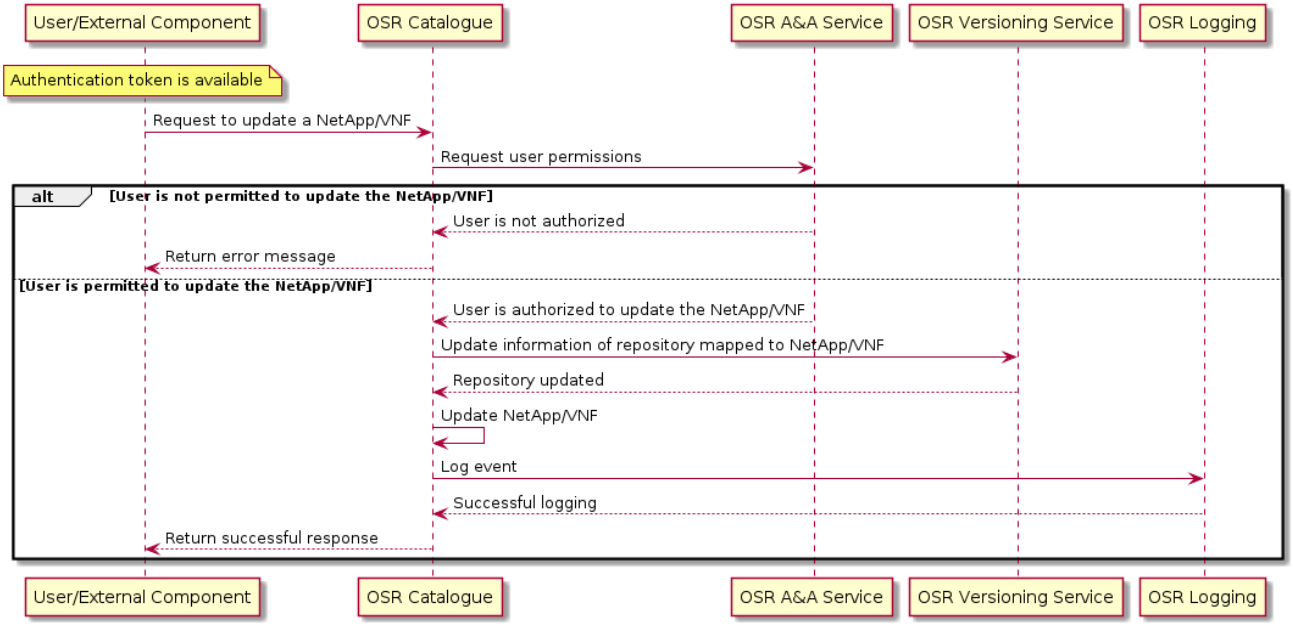

Figure 4-23 OSR Update NetApp/VNF

Delete NetApp / VNF

Deleting a NetApp/VNF is also a request to the Catalogue service. The Catalogue service communicates with the Code Versioning service to delete the NetApp/VNF project and with the Event Logging component to log the event.

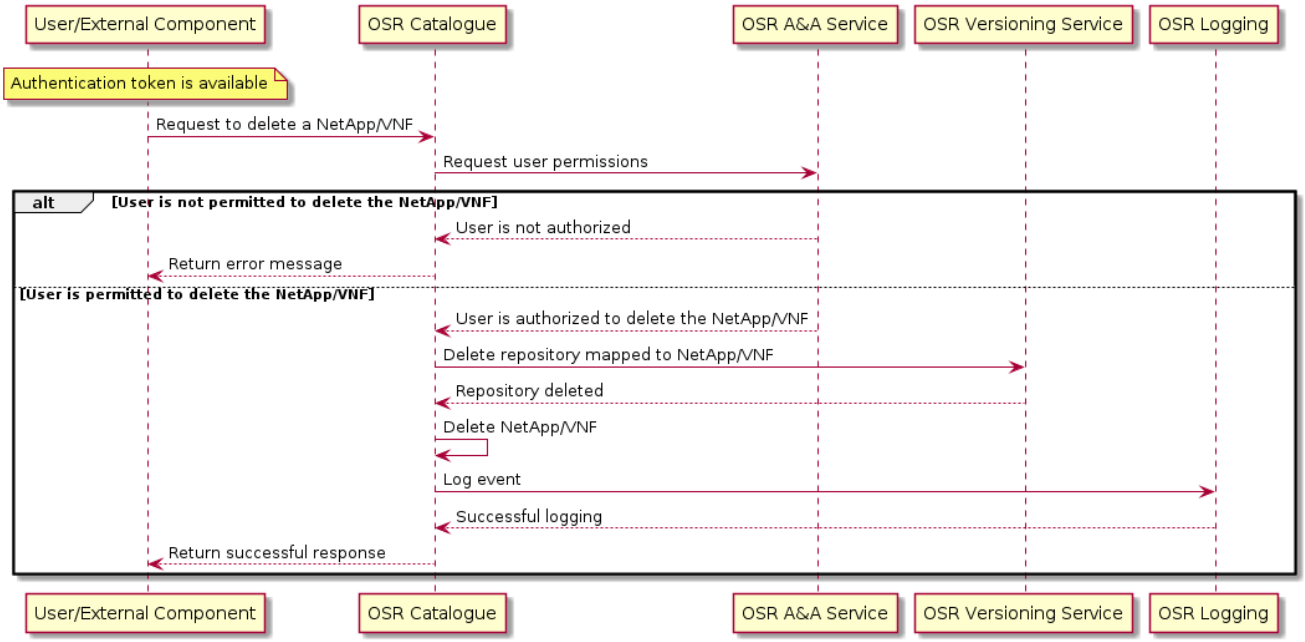

Figure 4-24 OSR Delete NetApp/VNF

Upload NetApp / VNF

The NetApp and VNF code are stored at the Code Versioning service. This request is directed to the Catalogue service and the Catalogue service forwards the files to the Code Versioning service. The event is logged in the Event Logger.

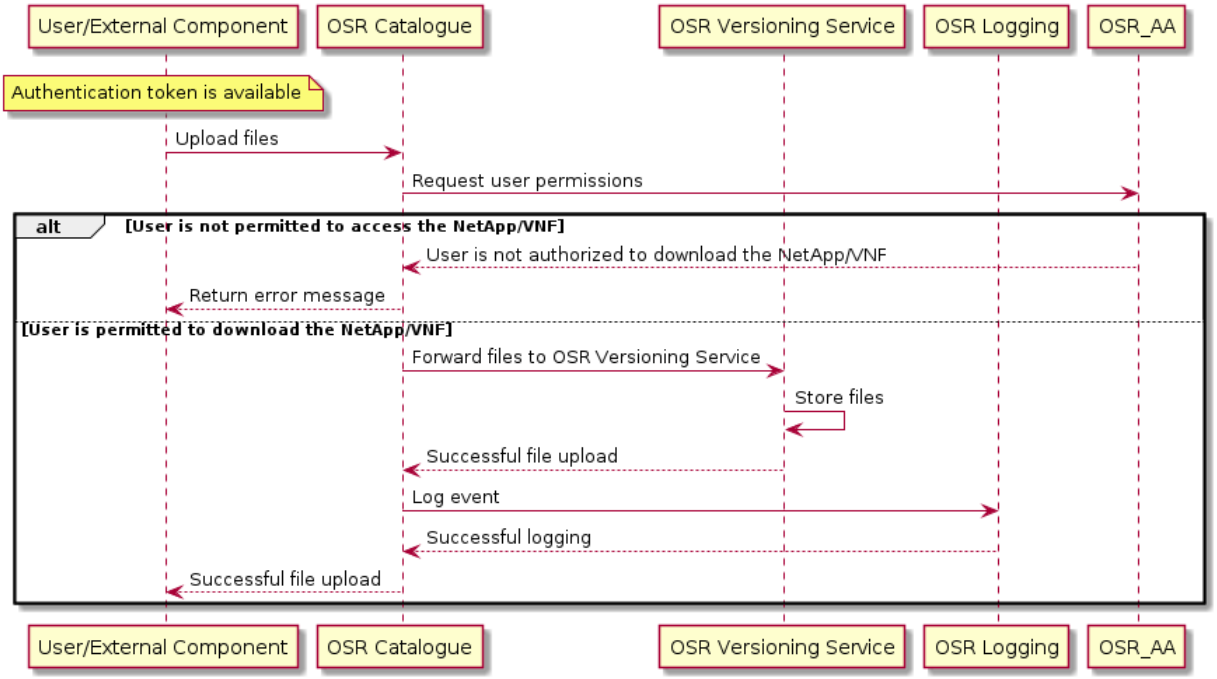

Figure 4-25 OSR Upload NetApp/VNF

Download NetApp / VNF

The download action is similar to the upload. In this case, the Code Versioning service generates a compressed file that contains all the NetApp or VNF code.

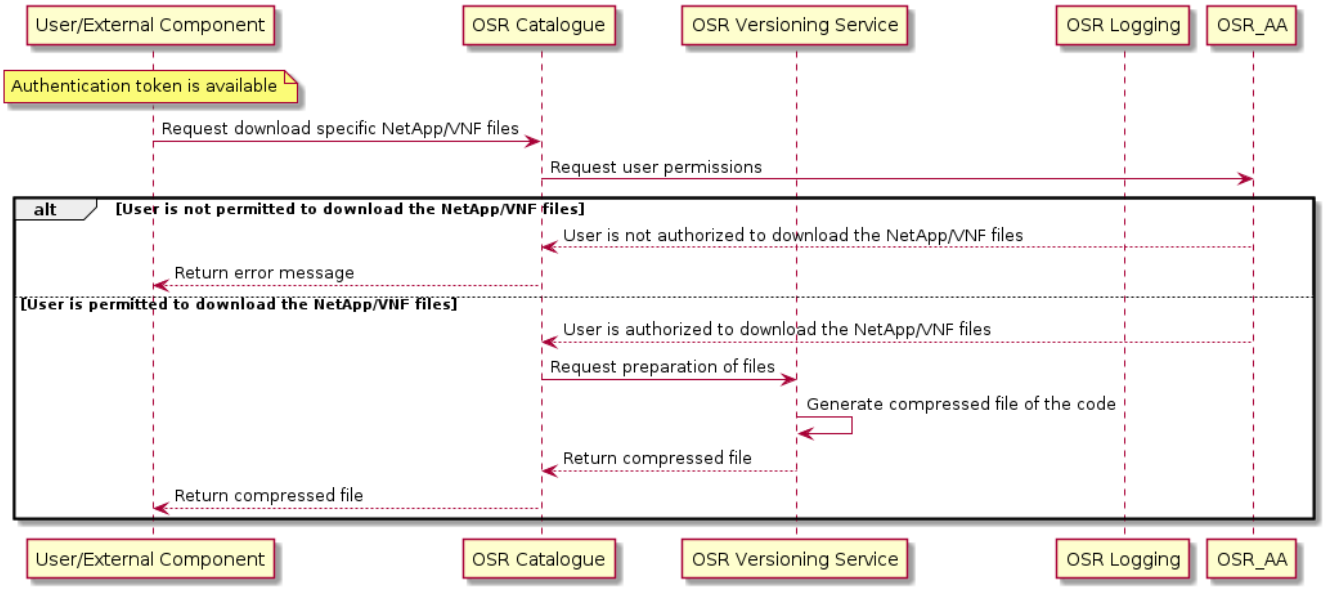

Figure 4-26 OSR Download NetApp/VNF

Show Event Log

A user can request a list of logs on a specific resource from the OSR. The request is sent to the Catalogue, and the Catalogue gets the user permissions from the A&A service. If the user can access the logs of the requested resource, then the list of the logs is returned.

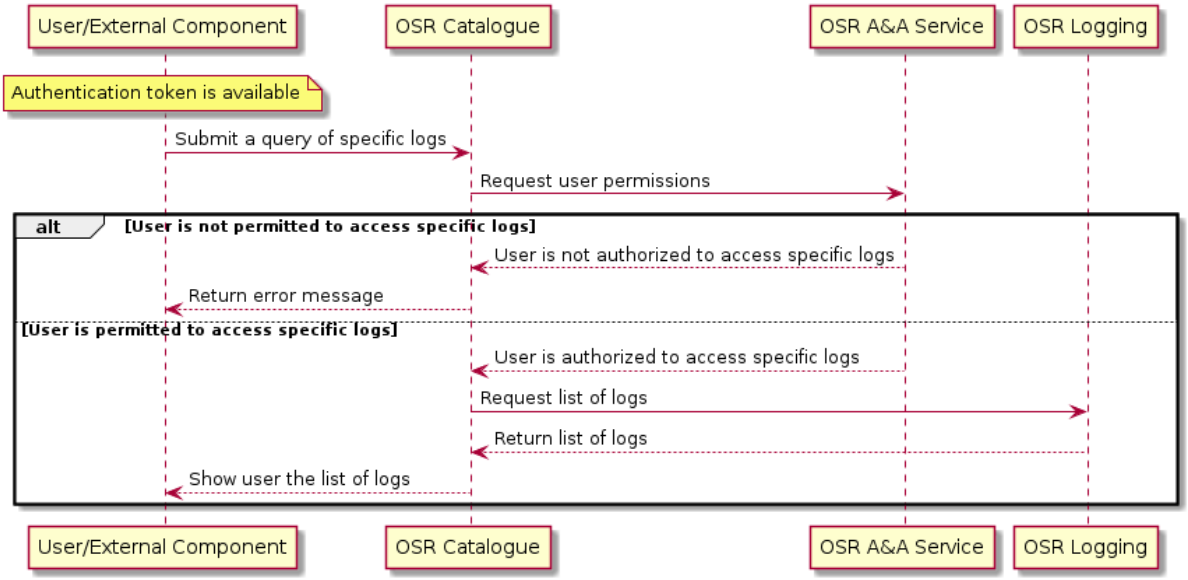

Figure 4-27 OSR Show Event Log

4.2.5 Security

The REST APIs of the OSR will be available to the public so the service uses HTTPS protocol to provide encryption to all requests.

4.3 V&V Framework

The V&V Platform will interact with several entities (Figure 4-28), namely the NetApp Developers, the OSR, and the M&O framework. The developers may be able to request just the verification or both verification and validation of their NetApps to accelerate the development of the VNFs and services. The OSR must request the verification and validation of a NetApp before it is stored in its own repository. To perform the validation process, the validation engine will request the onboarding and instantiation of NetApps, which will be terminated automatically once all the results and KPIs are gathered, to properly validate the NetApp.

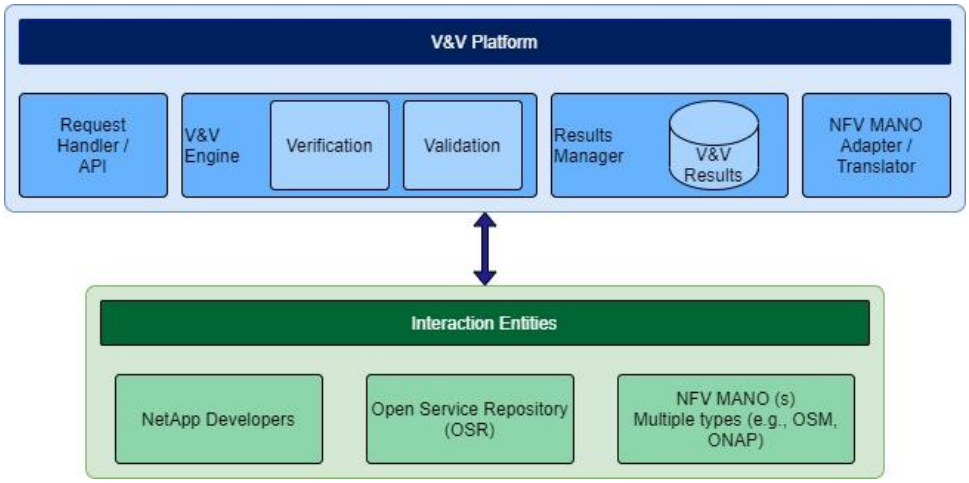

Figure 4-28 V&V interactions

4.3.1 Architecture

The overall V&V Platform architecture is depicted in Figure 4-29, showing the external entities that will interact with it. The internal architecture is composed by four main services, namely:

- API Request Handler: It is responsible for receiving and sending information to and from the users of the platform;
- V&V Engine: It is responsible for both the verification and validation processes of the NetApps;
- M&O Framework Adapter: It is designed to contact the Smart5Grid M&O framework in order to request onboarding and instantiation of NetApps;
- Results Manager: The entity that will store all the verification and validation results per each NetApp.

NetApp developers are the projected users of the platform. They can interact directly with the V&V Platform via Command Line Interface (CLI) or via the User Interface (Section 4.1), which uses the V&V API. The OSR will be interacting directly with the V&V API.

The V&V Engine is split into two sub-modules:

- Verification Engine: This will assess the syntax, the integrity, and the topology of the NetApps and/or VNFs.
- Validation Engine: This will address the onboarding and instantiation on the M&O framework and the KPI retrieval and validation.

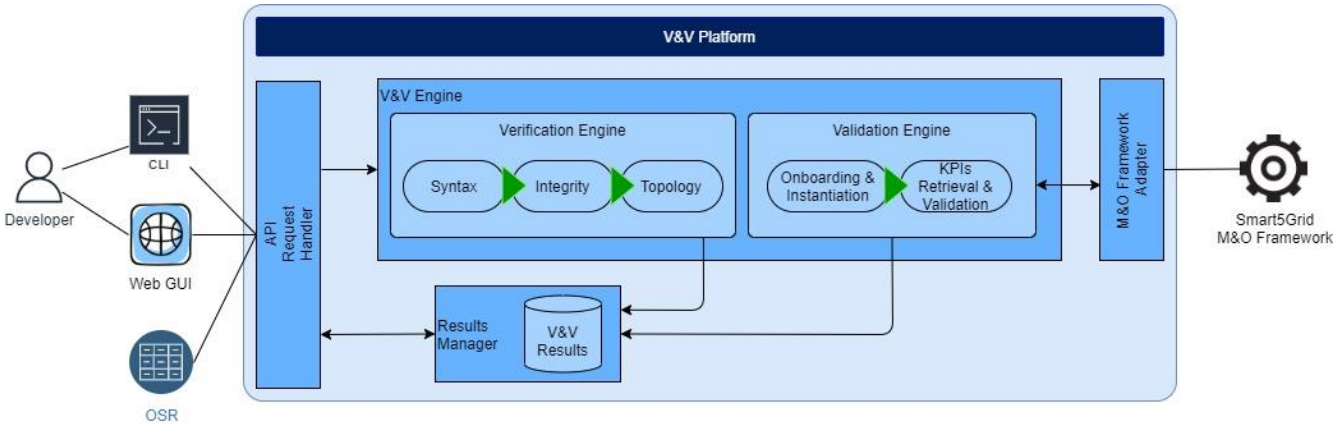

Figure 4-29 V&V Platform Architecture

The KPIs that should be retrieved for the validation of the NetApp are defined by the developer and are detailed in the NetApp descriptors. Each specified KPI must contain the metric (e.g., bandwidth, latency, jitter).

4.3.2 Functional description

This section will detail the Verification as well as the Validation processes of the V&V Platform, describing the procedures involved in each one.

4.3.2.1 Verification

The verification component of the V&V platform will address the composition of the Smart5Grid NetApp descriptors. It will provide the verification on the following elements.

- Syntax verification: The NetApp descriptor and corresponding VNF descriptors (VNFDs) are syntactically validated against the scheme templates specified by data model of Smart5Grid.
- Integrity verification: The validation of integrity verifies the overall structure of descriptors through the inspection of references and identifiers both within and outside the individual descriptors. As NetApp and VNFDs have different information scopes, the validation goals of this type of activity either in the context of a VNF or NetApp validation are provided as follows:
    - NetApp Integrity: NetApp descriptors typically contain references to multiple VNFs, which are identified by the ID of the VNF. The integrity validation ensures that the references are valid by checking the existence of the targeted VNFs. Integrity validation also verifies the connection points (CPs) of the NetApp. This comprises the virtual interfaces of the NetApp itself and the interfaces linked to the referenced VNFs. All CPs referenced in the virtual links of the NetApp must be defined, whether in the NetApp descriptor or in its VNFD.
    - VNF Integrity: Similarly, VNFs may also contain multiple subcomponents, usually referred to as the Virtual Deployment Units (VDUs) or Virtual Network Function Components (VNFCs). As a result, the integrity validation of a VNF follows a similar procedure of a

NetApp integrity validation, with the difference of VDUs being defined inside the VNFD itself. Again, all the CPs used in virtual links must exist and must belong to the VNF or its VDUs.

- Topology verification: This tool provides a set of mechanisms to validate the network connectivity graph to aid the development of connectivity logic. Typically, a NetApp contains several inter-connected VNFs and each VNF may also contain several inter-connected VDUs. The connection topology between VNFs and VDUs (within VNFs) must be analysed to ensure a correct connectivity topology. To present this rationale, Figure 4-30 depicts a NetApp example used to better illustrate validation issues. This figure is followed by a summary of the set of issues that this software can detect:

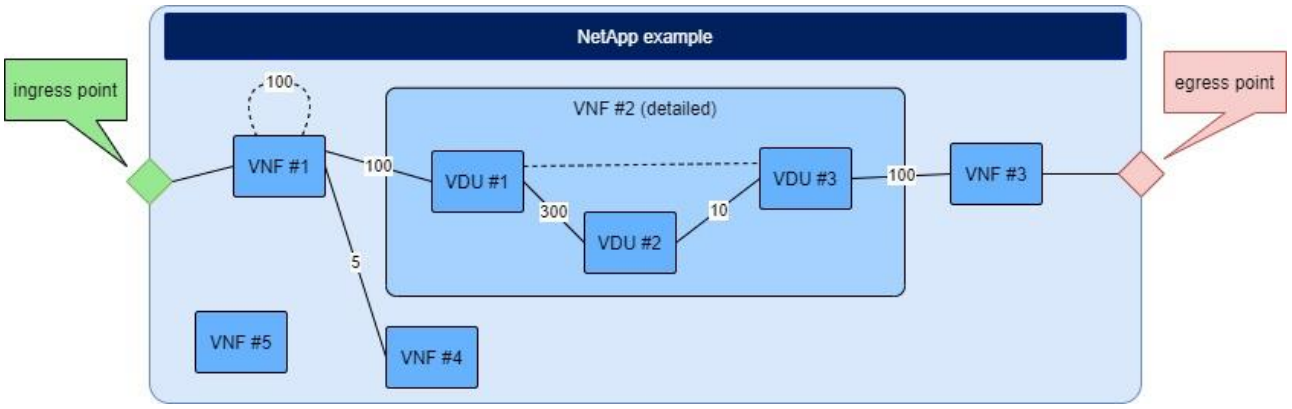

Figure 4-30 NetApp Components Example

- Unlinked VNFs, VDUs and CPs: Unconnected VNFs, VDUs and unreferenced CPs will trigger alerts to inform the developer of an incomplete service definition. In this case, VNF #5 would trigger a message to inform that it is not being used;
- Network loops/cycles: The existence of cycles in the network graph of the service may not be intentional, particularly in the case of self-loops. For instance, VNF #1 contains a self-linking loop, which was probably not intended. Another example is the connection between VDU #1 and VDU #3 which may not be deliberate. This tool analyses the network graph and returns a list of existing cycles to help the developer in the topology design. In this example, it would return the cycles:
  - [VNF #1, VNF #1],
  - [VDU #1, VDU #2, VDU #3, VDU #1];
- Node bottlenecks: Warnings about possible network congestions, associated with nodes, are provided. Considering the bandwidth specified for the interfaces, weights are assigned to the edges of the network graph in order to assess possible bottlenecks in the path. As specified in the example, the inter-connection between VDU #2 and VDU #3 represents a significant bandwidth loss when compared with the remaining links along the path.

4.3.2.2 Validation

The validation process comprises the deployment and instantiation of the to be validated NetApp in the M&O framework. In Smart5Grid, it is expected the V&V Platform to have the associated M&O framework to perform the NetApp validation tests which can be of multiple types as well (e.g.: OSM, ONAP, and others).

- NetApp onboarding: Once the translation process is finished, the next logical step is to onboard the NetApp in the corresponding M&O framework.
- NetApp instantiation: Here is where the Validation engine will request the instantiation of the NetApp.
- Retrieve KPIs: To properly validate the NetApp, the Validation engine will ensure that certain specified KPIs are met. Hence, the M&O framework will have a mechanism to measure and provide such metrics (more detailed in Telemetry Section 4.4.2.6). The KPIs to be assessed are specified by the developers in the Smart5Grid NetApp descriptors, as described in Section 4.6. The end-to-end latency of a NetApp, the latency between two VNFs or the bandwidth between two CPs are examples of KPIs that will be supported. The retrieved KPIs are then stored in the V&V results database for later analysis.
- Validation results analysis: This process verifies of the retrieved KPIs are within the thresholds specified by the developer. It is in this process that is determined if a NetApp is successfully validated.

4.3.3 Technical specifications

The V&V Platform architecture design will be independent and prone to be reusable in different projects and domains. Nonetheless, the platform will provide a Smart5Grid custom API service for accessing all its functionalities and it will provide different types of user roles and different authorizations for each role. For instance, the "developer" role will have distinct authorizations than the "OSR" role.

Another important aspect of the V&V Platform is the ability of providing V&V caching for the verification and validation results. Whenever a NetApp or a VNF is validated, it calculates the hash-ID that is unique for that particular artifact. This paradigm aims to significantly reduce the number of repetitive verifications and validations, which can be very resource demanding, particularly the latter. As an example, let us assume that a developer user requests a verification and validation of a NetApp and, after everything works well and obtains a successful validation, he decides to onboard it to the OSR catalogue. The OSR will also immediately request a verification and validation to the V&V Platform before storing it in its catalogue. As the V&V Platform already has a result in its database for that specific NetApp, it will not be validated twice, instead it will simply return the previously obtained result.

4.3.4 Interfaces and data to be exchanged

As mentioned before, the V&V Platform can be accessed and used by several parties. This section details the different workflows for each party in the Smart5Grid scope.

Developer requests a verification (only) of a NetApp

In the example shown in Figure 4-31, the developer requests the V&V Platform for the verification (only) of a NetApp. The depicted diagram steps are described as follows.

1. The developer requests the NetApp verification – for this, the Smart5Grid NetApp package, which include the NetApp descriptors, must be sent to the V&V Platform.

2. The V&V Platform generates a unique hash-ID based on the uploaded package checksum (MD5[22] or SHA1[23] will be used, not yet defined).
3. The generated hash-ID is provided to the developer for later reference.
4. The V&V Platform issues the Verification Engine the verification of the NetApp.
5. Syntax is verified.
6. Integrity is verified.
7. Topology is verified.
8. All results are stored in the Results Manager database for the generated hash-ID.
9. The developer requests the results from the verification based on the provided hash-ID.
10. 11. and 12. The results are retrieved from the Results Manager and provided to the developer.

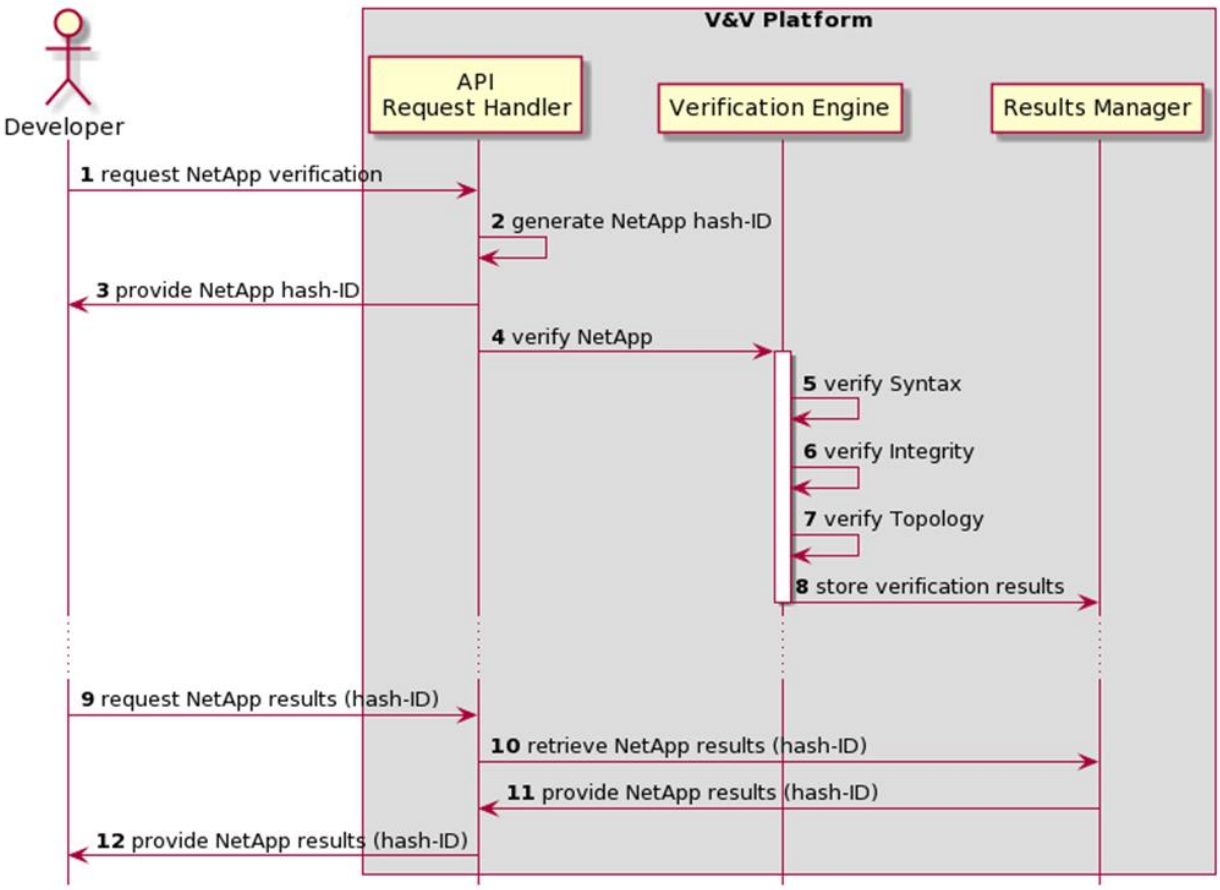

Figure 4-31 Developer requests a verification of a NetApp

[22] The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database. For further information also see, for example: https://en.wikipedia.org/wiki/MD5

[23] In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard. For further information also see, inter-alia: https://en.wikipedia.org/wiki/SHA-1

Developer / OSR requests a verification and validation of a NetApp

Figure 4-14 shows the process that takes place when either the developer or the OSR request the V&V Platform for the verification and validation of a NetApp. The depicted diagram steps are described as follows:

15. The developer/OSR requests the NetApp verification and validation – for this, the Smart5Grid NetApp package, which include the NetApp descriptors, must be sent to the V&V Platform.
16. The V&V Platform generates a unique hash-ID based on the uploaded package checksum (MD5 or SHA1 will be used, not yet defined).
17. The generated hash-ID is provided to the developer for later reference.
18. The V&V Platform issues the Verification Engine the verification of the NetApp.
19. Syntax is verified.
20. Integrity is verified.
21. Topology is verified.
22. The verification results are stored in the Results Manager database for the generated hash-ID.
23. The Verification Engine issues a successful verification.
24. The V&V Platform issues the Validation Engine the validation of the NetApp.
25. 12. 13. 14. The Validation Engine performs the onboarding of the NetApp Service Package.
1. 16. 17. 18. The Validation Engine requests the instantiation of the NetApp Service.
15. 20. 21. 22. Execution KPIs are retrieved.
19. Validation results are stored in the Results Manager database for the generated hash-ID.
20. 25. 26. 27 Developer/OSR requests the results from the verification and validation based on the provided hash-ID which are provided.

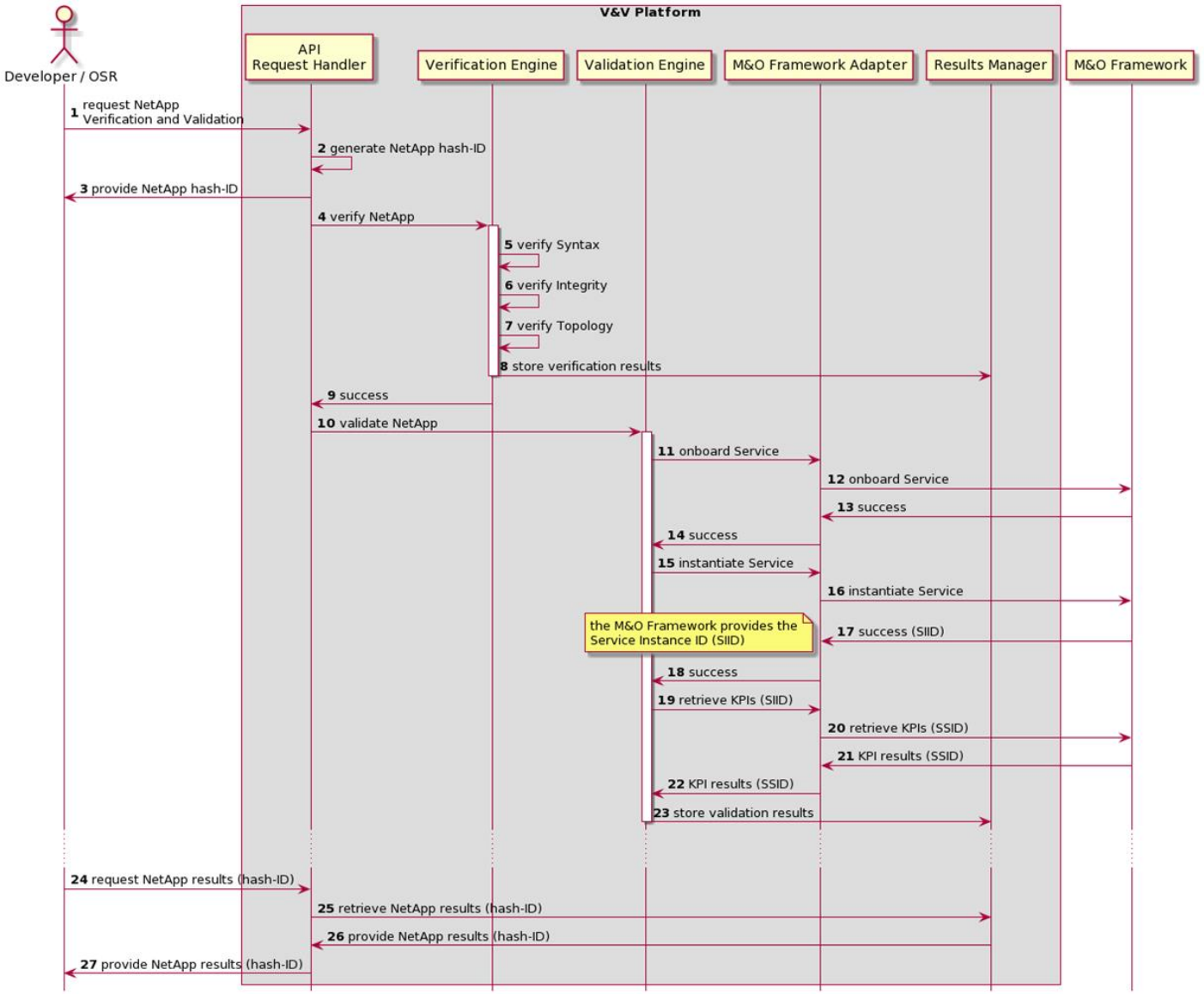

Figure 4-32 Developer/OSR requests a verification and validation of a NetApp

4.3.5 Security

Regarding security, one of the most important aspects is to ensure that there is no tampering or impersonation in the interactions with the V&V Platform API. To prevent such events and be able to provide Authentication, Authorization and Accounting (AAA), the Platform will be designed to rely on a third-party identification technology, such as Keystone [63]. On top of that, all communication channels will use HTTPS with industry standards for authorization, most likely OAuth 2.0[24].

Another key aspect pertaining to the security of the V&V Platform is to enforce a secure commutation channel between the V&V Platform and the several M&O frameworks. This specification is still an ongoing work, however, apart from HTTPS, Virtual Private Network (VPN) tunnels (e.g.: OpenVPN or IPsec) are a possibility, especially in the likely event that it is necessary to traverse through a firewall placed on the Telco Core Network perimeter.

4.4 Management and Orchestration Framework

The M&O framework gathers the set of architectural elements in charge of supervising and coordinating the operations and lifecycle of the telecommunication network's virtualized communication/storage/computing resources, VNFs, and services. Such functionalities include:

- The deployment, inventory, and management of the Network Function Virtualization Infrastructure (NFVI).
- The onboarding, placement, scaling, migration, upgrade, and termination of VNF instances, including the dynamic orchestration of VNFs across different physical sites (e.g.: edge and central clouds).
- The design, instantiation, and maintenance of communication services and NetApps.
- The monitoring, collection, and forwarding of performance measurements and events among the involved architectural blocks and functional elements.
- The enforcement of security across different elements and architectural layers.

From the 5G networking perspective, the M&O framework is responsible for the coordination of network slices over which communication services and NetApps are instantiated. Namely, this involves:

- The management of instantiation requests of communication services and NetApps.
- The transformation of service and NetApp requirements into resource requirements.
- The assignment of network resources to Network Slice Instances (NSI).
- The lifecycle (preparation, instantiation, configuration, activation, run-time, and decommissioning phases), policy, and fault management of the NSIs over which communication services and NetApps are deployed.
- The coordination of the sharing of network slice constituents and VNFs among multiple parties or, vice versa, the support of mechanisms that guarantee resource separation and isolation.

[24] OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This specification and its extensions are being developed within the IETF OAuth Working Group. For further information also see: https://oauth.net/2/

4.4.1 Architecture

Altogether, the M&O layer of the Smart5Grid platform merges into a unified framework a number of functionalities that are part of two frameworks: ETSI NFV MANO [61] and 3GPP´s 5G network slice management [48].

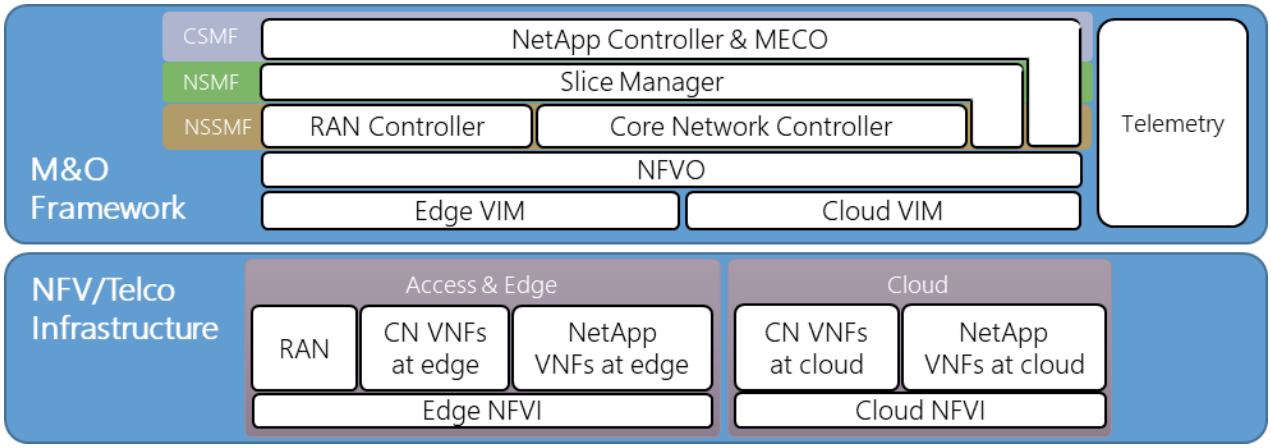

Figure 4-33 The NFV/Telco layer of the Smart5Grid architecture

Figure 4-33 provides a general overview of the main blocks that compose it. As shown, it includes the main constituent blocks of the M&O framework and the underlying NFV and telecommunication infrastructure:

- The NetApp Controller & Multi-access Edge Computing Orchestrator (MECO), cf. Section 4.5.2.1 NetApp Controller & MEC Orchestrator.
- The SM, cf. Section 4.5.2.2 Slice Manager (SM).
- The NFV Framework, including Network Function Virtualization Orchestrator (NFVO) and the VIMs of the cloud and edge resources, cf. Section 4.5.2.3 NFV Framework.
- The CN Controller, cf. Section 4.5.2.4 5G CN Controller.
- The RAN Controller, cf. Section 4.5.2.5 RAN Controller.
- The Telemetry module, cf. Section 4.5.2.6 Telemetry.

The NetApp Controller & MECO, the SM, the RAN Controller, and the CN Controller provide all the functionalities related to the network slice management described above. As further explained later on, they overall supply a set of functionalities that 3GPP entrusts to the Communication Service Management Function (CSMF), the Network Slice Management Function (NSMF), and the Network Slice Subnet Management Function (NSSMF). In addition, coherently with the ETSI NFV MANO paradigm, the NFVO and the VIMs oversee the VNF and NFVI handling and coordination. Moreover, the Telemetry module superintends the gathering and exchange of performance and monitoring data for analytical purposes. These data can be used for network optimization and fault management. Finally, the M&O layer is directly interconnected with the V&V framework for the instantiation of NetApps for validation purposes (cf. Section 4.4 V&V framework and Section 4.5.2.1 NetApp Controller & MEC Orchestrator).

4.4.2 System Level Components

4.4.2.1 NetApp Controller & MEC Orchestrator

The NetApp Controller & MECO has the role to manage the NetApps and MEC servers' lifecycles. This includes NetApp-specific functions like NetApps deployment, migration, termination, set and forward the required traffic routing rules, but also functions like node (re-)provisioning and configuration. Since this is the component that decides where a NetApp should be deployed, it is usual that the MECO has a broader view than just the edge, and it usually can manage resources ranging from the far and near edge to public and private data centres.

Although distinct, some of tasks performed by the MECO are tightly related and complementary to the functionality of the NFVO described in Section 4.5.2.3. Due to this fact, some MECO solutions can also perform NFVO functions.

4.4.2.1.1 FUNCTIONAL DESCRIPTION

Since the NetApp Controller & MECO offers different functionalities, it comprises different internal parts that can be grouped into the following components:

- Node Provisioner: This is the component that allows to configure and register new nodes into the MECO over the network offering a near Zero-Touch Provisioning (nZTP) experience. Once a node is provisioned or registered, it is added to the list of available nodes and the controller starts to monitor it and to consider it to deploy NetApps. When provisioning a node, users can select how the node is going to be configured selecting from a list of configurations such as OS (e.g., CentOS 7.9 [64] with Kubernetes All-in-one configuration [65]) or selecting which cluster the node should be added to. The node provisioner will take care to properly register the node to the cluster masters. This component also offers the possibility to add nodes, or even entire clusters, that are already provisioned.
- Placement Advisor: This is the component that suggests a good placement for every component of a NetApp instance specifying how many resources (i.e., CPU cores, DRAM, etc.), and which resources (e.g., cpuset=13-17 of node node-uuid).
- Monitoring System: This is the component that actively scrapes the endpoint of orchestrator's node agents and NetApps to collect and monitor metrics and events about the servers but also about the NetApps. Usually, this component comprises a time series database where the metrics are stored in real time at given intervals. Additionally, this component can be used to trigger alerting whenever needed (e.g., to trigger NetApp migrations) and to create a real-time monitoring dashboard.
- System Frontend: This is the component used by external parties to communicate and operate with the NetApp Controller and MECO.
- Orchestrator: This is the core component that coordinates NetApp deployment, migration, and termination among the many components of the MECO and external components. For example, this is the component that communicates with the NFVO and the VIM to deploy or terminate a NetApp instance, interfaces with the SM, and instructs possible third-party AF about the traffic routing rules needed.

4.4.2.1.2 TECHNICAL SPECIFICATIONS

Since the NetApp Controller and MECO is composed of different components, it is advisable that it follows a microservice architecture using containers. Container-orchestration systems like Kubernetes can be used to automate the deployment, scaling, and management of the different components. Finally, the communications between the various components should use a reliable message delivery system that offers persistency. Apart from these general considerations, below we discuss the technical specifications of each individual component:

- Node Provisioner: When provisioning a node using nZTP to provision remote nodes over the network, the user needs to preload a custom iPXE (Pre-boot eXecution Environment) ISO[25] (Optical Disc Image) in the system BIOS (Basic Input/Output System) and boot that ISO. At boot, the software executed contacts the controller to begin the automated provisioning over an encrypted channel. During the provisioning phase, the OS is installed alongside with the required drivers, security patches, encryption keys, secure communication tunnels, and the VIM. Finally, this component also installs some software (e.g., collectd [66], iperf [67], cloudprober [68], Kubernetes Node Feature Discovery [69], Ansible facts [70], etc.) – called node agents – to extract system configuration and metrics such as resource utilization, network latency, and bandwidth. When needed, the Node Provisioner can also register nodes already provisioned by skipping the initial OS installation.
- Placement Advisor: To find a good placement, the Placement Advisor can take into consideration different factors that can depend on the MECO configuration and deployment. Common factors that should be always considered are NetApp minimum resources (CPU cores, DRAM, disk size, specific HW feature, etc.), target Service Level Objective (SLO), and traffic routes. A non-exhaustive list of more elaborate factors that can provide a better placement includes known performance fingerprints of the NetApp, affinity and anti-affinity patterns with other hardware and software components, network congestions, etc. This second list requires to have record of previously deployed NetApps or additional input from the users.
- Monitoring System: To monitor node and network events and metrics, this component comprises one or more time series databases (e.g., Prometheus) where the metrics are stored in real time at given intervals. Independently from which time series database is used, the metric collection should follow the idea that applications or node agents publish their metrics using HTTP endpoints (e.g., localhost:9090/metrics) and it is up to the database to scrape such target endpoints one after the other. That is, when more and more target endpoints are added, the database decreases the scraping frequency of each endpoint, preventing data congestion on the database. Using the time series databases, the monitoring system can offer interactive dashboards with charts and graphs to monitor NetApps Service Level Indicators (SLIs) and resource utilization of the nodes. Furthermore, the monitoring system needs a way to add new targets and remove old. This allows the Orchestrator to add and remove monitoring targets when a NetApp is deployed and undeployed. The same applies for adding and removing monitoring targets for node agents when a node is provisioned or discontinued. For what concerns the monitoring part, the database does not simply scrape and store metrics, but also it must be able to continuously evaluate such metrics and trigger alarms when a metric is outside the expected values. Similarly, to the scraping

[25] An ISO file, also known as an ISO image, is a file that contains all the installation files for a single program. Certain software programs, especially large ones, are sometimes made available as ISO files, including Microsoft Office and the Windows operating system.

endpoints, the monitoring system should allow adding, editing, and deleting the evaluation expressions required by the NetApps. These expressions are the criteria used to analyse aggregated metrics and can be simple comparisons (e.g., higher than) or more complex human-readable expressions that aggregate data over time. As an example, Prometheus allows to evaluate the 99th percentile of a metrics called latency over the last 5 minutes with a simple expression like: latency[5m]{quantile="0.99"} [71].

- System Frontend: This component includes a web Graphical User Interface (GUI) that users utilize to operate the NetApp Controller & MECO and the API exposed to the V&V framework used for the validation of NetApps. Furthermore, the System Frontend includes a suite of services for authentication and authorization like an Identity and Access Proxy (IAP), Identity Management, Access Control Server, and an OAuth 2.0 and OpenID Connect provider (e.g., Ory ecosystem [72]).

4.4.2.1.3 INTERFACES AND DATA TO BE EXCHANGED

This section contains the description of the data extracted from the NetApp descriptors, the OSR interface that is referenced in the NetApp descriptor, as well as the traffic policies and the SM.

Data extracted from NetApp Descriptors

When deploying a NetApp, the NetApp Controller and MECO will use the NetApp Descriptors to extract the following information:

- The list of VNFs, and per every VNF:
  - The reference to the containerized VNF stored in the OSR.
  - Minimum resources required. If no minimum resources are specified, the VNF will executed using a best-effort approach without guarantees.
  - The list of metrics endpoint used to scrape and monitor the NetApps SLIs.
  - The list of required traffic routing rules.
- The list of SLI with their target SLO.

Interface with the OSR

Whenever a NetApp is being deployed on a node, the NetApp controller will use the OSR references extracted from the NetApp descriptor to clone all required docker image from the OSR to the nodes or to the NetApp controller's own docker registry. No further integration between the OSR and the NetApp Controller and MECO is required.

Traffic policies and Slice Manager

Regarding the traffic policies, these are extracted by the NetApp Descriptor and are then combined with the address of the deployed NetApp instances to obtain the actual rule. Once the rules for a NetApp are fully defined, the NetApp Controller and MECO uses an AF to forward the traffic rules to the 5G core. When forwarding traffic rules, as per 3GPP TS 29.502 [73], the MECO uses the AF to talk to the 5G Core Network Exposure Function (NEF) to setup the needed Packet Flow Description (PFD). Then, as per 3GPP TS 23.502 [74], the AF creates the traffic influence rules requesting a Data Network Access Identifier (DNAI) change notifications to know that the traffic rule has been forwarded to the User Plane Function (UPF).

For what concerns the integration between the NetApp Controller and MEC Orchestrator with the SM, the NetApp Controller and MEC Orchestrator forwards requests to create, edit, and delete a slice. Upon a

request, the SM interacts with the resource controllers (i.e., VIM/RAN/TN/5GCN Controllers) to carry out the request and finally respond to the NetApp Controller and MEC Orchestrator with information about the slice or the occurred errors.

NetApp Monitoring the edge->core

Monitoring the status of a NetApp is crucial to provide correct service quality. The monitoring should not only check if a NetApp is "up and running", but also it should also make sure that the NetApp SLIs, or KPI, are meeting the Service Level Objective (SLO) set for a NetApp instance. This requires two efforts from NetApp providers. Firstly, they must expose a way to extract the real-time value of their SLI. Secondly, they must instruct the NetApp Controller and MEC Orchestrator on how to collect, analyse, and react whenever an SLO is being breached. While the first effort is about creating an HTTP endpoint, the second is to provide a NetApp descriptor that describes: HTTP endpoints, expression to evaluate every SLI, and the instructions to follow when a SLO is being breached (e.g., migrate service, change the number of resources allocated, etc.).

Figure 4-34 shows the sequence diagram of a NetApp deployment and monitoring. This diagram offers a simplified view, where the NetApp Controller and MEC Orchestrator are considered as one. To see how the internal modules of the NetApp Controller and MEC Orchestrator interact with each other when deploying and monitoring a NetApp, refer to Figure 4-35. The main actors involved in these scenarios are described below:

  - Deployers: All actors and internal components that can deploy NetApps, human and not. In the case of a human actor, they will interact with the web UI of the NetApp Controller and MEC Orchestrator. Instead, in the case of a non-human actor, this can interact via the API offered by the MEC Orchestrator.
- NetApp Controller and MEC Orchestrator: Since MEC Orchestrator is composed of many components, so not to lose the focus, we only look here at the interactions between the three most relevant of them, and we group the other components together under a collection - Others MECO Components (e.g., AF):
  - Placement Logic: The component that decides which placement – how many resources and which ones – is assigned to every component of every NetApp instance.
  - Orchestrator: The core component that coordinates NetApp deployments and migrations. It is also the central entity that interfaces with the many components of the MEC Orchestrator and external components.
  - Monitoring System: Component that actively scrapes NetApps endpoints to collect and monitor their metrics and events. Additionally, this component can also be used to trigger alerting whenever needed (e.g., to trigger NetApp migrations).
  - Others MECO Components (e.g., AF): All the components of the MEC Orchestrator not described above.
- NetApp: As far as it concerns monitoring, a NetApp that exposes its metrics should be seen as two different entities: its Service Logic and its Metrics Endpoint. Independently of how they are implemented (i.e., as different threads of the same process, as different processes inside the same container, or as different containers), it is important to make the following distinction:
  - Service Logic: The core logic of the service offered by the NetApp.
  - Metrics Endpoint: The endpoint that exposes the real-time value SLIs of the service logic.

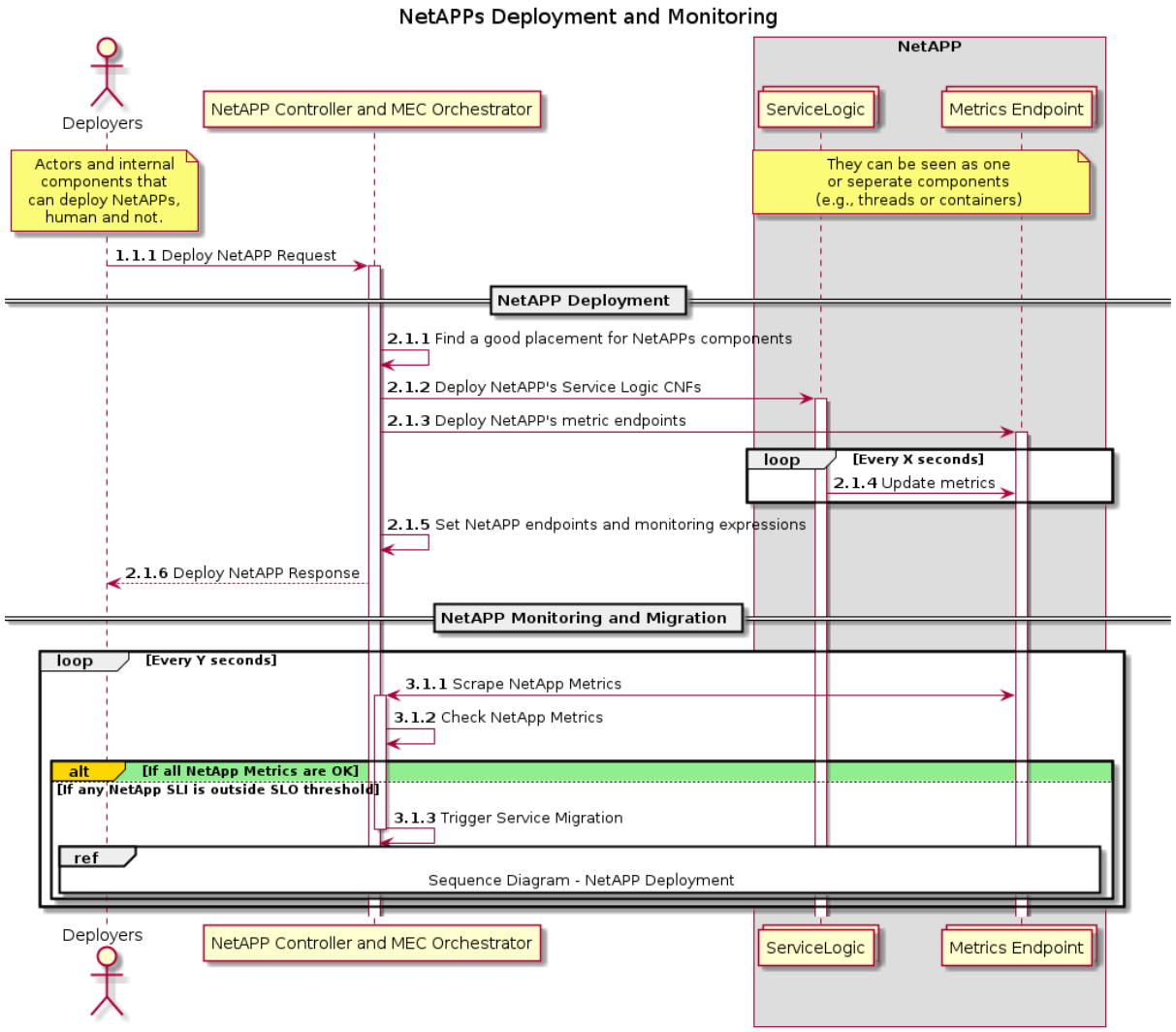

Figure 4-34 UML Sequence Diagram regarding the NetApp deployment and monitoring use case

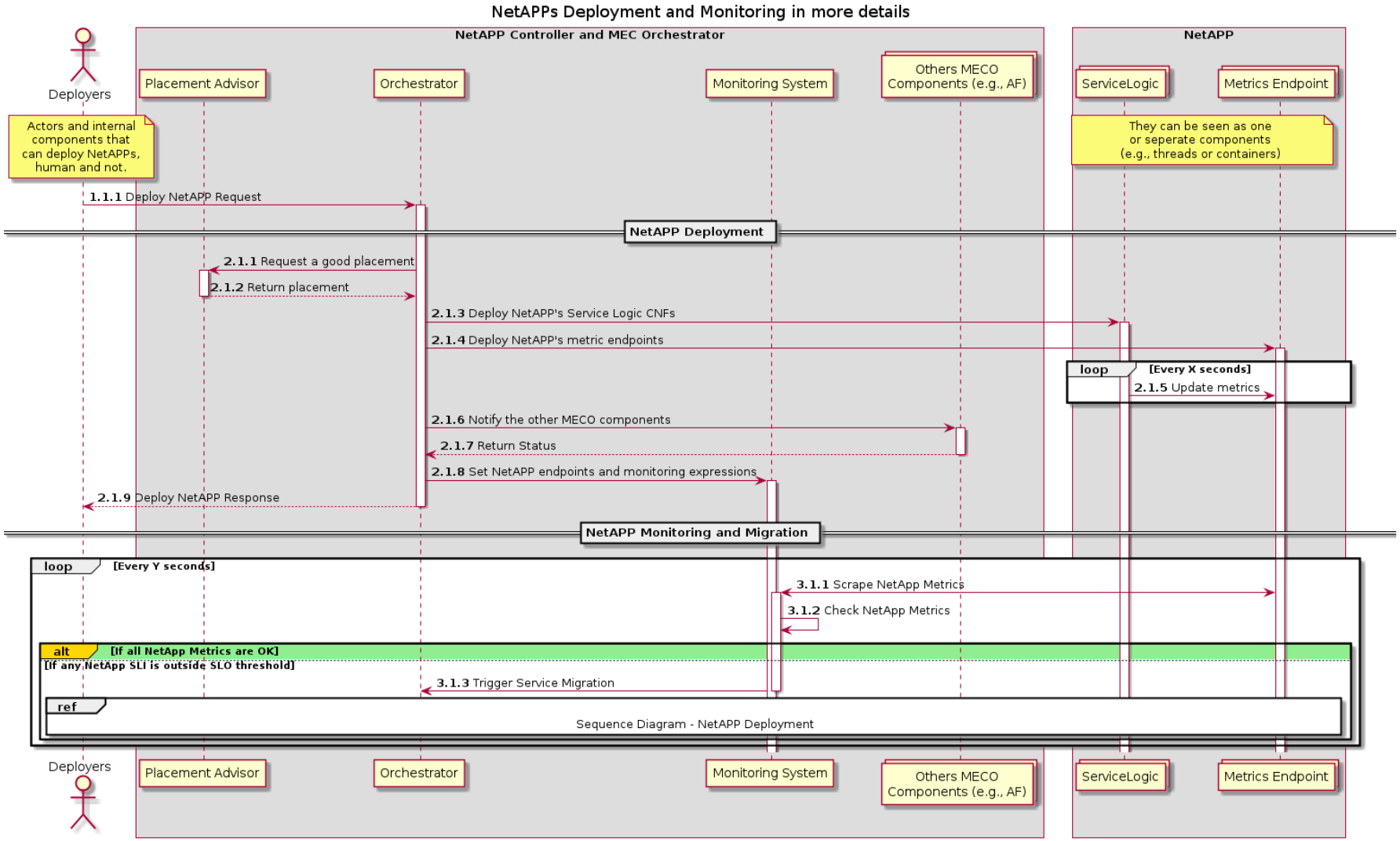

Figure 4-35 Sequence Diagram regarding the NetApp Deployment and monitoring with more details

4.4.2.1.4 SECURITY

To offer reliable security protection, it is of paramount importance that no component uses custom authentication method, hashing functions, and services. Instead, it is advised to use open-source components that are implemented by security experts and apply security standards established by experts like National Institute of Sciences NIST, Internet Engineering Task Force (IETF), known research institutes, etc.

- General Security Measure for Controller and Nodes:
  - On bare metal nodes, simultaneous multithreading implementation such as Intel's Hyperthreading [75] should be disabled to prevent the exploitation of CPU bugs like Spectre and Meltdown[26].
  - It is suggested to use platforms, either bare metal or virtualized, that offer a recent implementation of Trusted Platform Module (TPM, also known as ISO/IEC 11889 [76]). TPM main scope is to ensure that devices boot using a trusted combination of hardware and software.
  - Simultaneous multithreading implementation such as Intel's Hyperthreading will be disabled to prevent the exploitation of CPU bugs like Spectre and Meltdown.
  - When deploying HW nodes, it is possible that such nodes come equipped with a Global Positioning System (GPS) receiver that looks the node from booting if outside a designated region.
- Controller security:
  - All connections to the controller will use TLS 1.2 or higher – prior versions are deprecated.
  - Furthermore, incoming request should be shielded by a zero trust IAP, which authenticates and authorizes all incoming requests.
  - User login and registration requests will be forwarded to an Identity Management that stores users and password in a data base. Passwords will be encrypted using hashing functions (e.g., bcrypt[27]) that incorporate salts to protect against rainbow table attacks and that offer protection to brute-force attacks.
  - To offer different kind of user roles (e.g., simple user, administrator, et cetera) the controller will use an authorization system that allows to define Access Control Policies.
  - Logging into the OS hosting the controller will be allowed only via SSH (Secure Shell) using keys as authentication method and only from known IPs.
- Node Security:
  - When available, nZTP will be fully encrypted. This is achievable by shipping nodes with a custom IPXE ISO image that is used at the first boot.

[26] Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. For further information also see, for example: https://meltdownattack.com/

[27] bcrypt is a password-hashing function designed by Niels Provos and David Mazières, based on the Blowfish cipher and presented at USENIX in 1999. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power. For further information see, among others: https://en.wikipedia.org/wiki/Bcrypt

  - If a node is provisioned via the controller, every OS package should be retrieved by the controller itself and not from public packages resources. This helps to control the version of installed packages and full control on which updates are installed.
  - When a node is registered to its container, Intelligent Platform Management Interface (IPMI) credentials will be added to the container. This allows shutting down and reprovisioning a node, and so take back control, if there is the suspicion that the node has been breached.
  - Logging into nodes will be allowed only via SSH using keys as authentication method and only from the controller. SSH connections from other nodes will not be allowed.
- Communication Security:
  - To encrypt the communication between the nodes and the controller, all communication should go via encrypted tunnels. Such tunnels shall be established as soon as possible which means either while provisioning the node, or as first thing after an already provisioned node is registered to the controller. Obviously, these encrypted tunnels come with a toll on CPU cycle, but they are a necessary measure to protect the traffic.

4.4.2.2 Slice Manager (SM)

The design, deployment, and management of virtualized services over distributed environments is a non-trivial task. The orchestration of these services, which can span multiple network segments (radio, transport, clouds), is the responsibility of a specific module that takes care of the coordination of the infrastructure and network resources to ensure the end-to-end communication. Within the Smart5Grid architecture, the SM oversees performing these complex tasks. In the following sections the features, functional aspects and technical specifications are described.

4.4.2.2.1 FUNCTIONAL DESCRIPTION

The SM is one of the key elements that guarantee the management and orchestration of the infrastructure resources, as well as the NetApp service deployment in an agile way. The SM performs the logical partition in each resource offered by the infrastructure owner (RAN, Compute, Transport, and 5G CN). Those logical partitions, simply named as a collection of chunks, represent an NSI which considers the service requirements specified by the customer. In detail, this component allows the following functionalities:

- The dynamic provisioning of end-to-end network slices, both at infrastructure level (infrastructure chunks) as well as at network level (networks chunks), bearing in mind the performance requirements per slice, such as QoS policies.
- The clients and third parties to handle the network slices LCM in an agile manner in terms of commissioning, deployment, fault, and configuration procedures performed over the chunking resources and the NSs.
- The interaction with VIM technologies for the management of edge/cloud infrastructures such as OpenStack to provide better support of multi-tenancy and multi-tier services. Also, it interacts with NFV MANO frameworks, such as OSM, to coordinate the network services LCM procedures in a multi-tier mode.
- Seamless and dynamic network service provisioning at the network level by establishing the service chain communication among several network functions, which together describe a NetApp. These NetApps could be distributed along the multiple infrastructure domains.

- A flexible interaction with O-RAN [77] aligned access networks to enable a transparent and dynamic resource orchestration of the multiple wireless devices such as small-cells, Wi-Fi networks and 5G-NR (New Radio).

According to the Smart5Grid architecture, SM module is located at the NFV/telco layer inside of the M&O framework. In this architecture, the SM interacts with multiple modules. For instance, at the southbound interface (SBI), SM communicates with the RAN Controller, the 5G CN Controller and the VIM to reserve infrastructure and network resources during the slice instantiation process [78]. Similarly, with this interface, the SM delegates to the NFVO the network service deployment on a specific slice in terms of VNFs by using descriptors onboarded previously. Finally, it configures the chunk resources to accomplish with the end-to-end service communication requirement. On the other hand, through the northbound interface (NBI), the SM exposes the information related to the users, infrastructure/network resources, slices instantiated in terms of chunks and NSs deployed on each slice. Therefore, the NetApp Controller using this interface can design and deploy the slice services in terms of blueprints made available by network operators. It can also control and orchestrate their associated resources. The main procedures of each interface are described in more detail in Section 4.4.2.2.2.

Figure 4-36 illustrates the key functional procedures carried out by the SM following a network slice instantiation request. First, the SM reads and identifies the slice parameters passed by the NetApp Controller to translate them in terms of infrastructure resources. The SM interacts with the RAN/5G CN Controllers and the VIMs to validate and assign infra-resources to the slice. The slice information is stored in a centralized database. Subsequently, the NetApp Controller and NFVO systems can perform the management and orchestration procedures. In fact, they can create, deploy, and monitor the NetApp services belonging to a slice that could span different domains (e.g.: edge/cloud computing). In Section 4.4.2.2.3, the NetApps deployment workflow is described in depth.

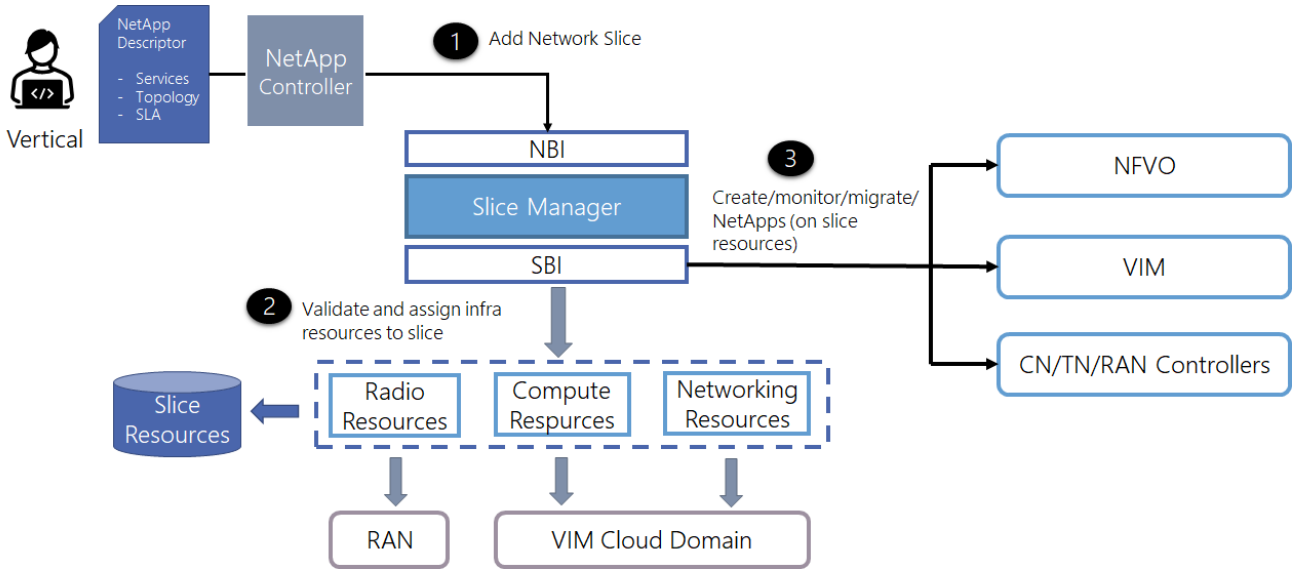

Figure 4-36 Functional role of the SM in Smart5Grid platform

It is worth noting that the main role of the SM in every UC is to preserve the logical isolation between the different slices while ensuring the requirements expected by the slice users. The slicing model performed by the SM is based on the 3GPP approach and the Next Generation Mobile Networks (NGMN) [79] Alliance´s slicing concept, which includes the radio part as well.

The SM follows concrete steps for handling the preparation, fault, instantiation, configuration, service provisioning, service update, and service recovery procedures per network slice instantiation. These procedures are performed by means of its REST-based API interfaces through the interaction with the rest of Smart5Grid architectural modules at M&O framework (NFV/Telco layer). The operational flows executed by the SM can be summarized as follows:

- Management of infrastructure resources: It is related to the process of registering infrastructure resources. For example:
  - Cloud/Edge Compute Registration: Performed through the interaction with VIMs.
    - Compute resource object stored in the SM.
    - API compute information to be reached from SM.
    - External networking object belonging to infra-cloud stored in the SM.
  - RAN Registration: Performed through the interactions with RAN controller.
    - Cell Creation/configuration
    - Devices/interfaces configuration
    - RF/ports configuration
- Management of reserved infrastructure (chunks): These operational flows perform the registration and configuration procedures on the resources reserved per slice.
  - Cloud/Edge Compute Chunks:
    - Assigned Compute chunk stored in SM.
    - Related-slice users and project created in NFVO.
    - VIM account registered in NFVO.
  - RAN Network Chunks:
    - Retrieval information of RAN topology configured previously.
    - Validation of RAN resources.
    - Radio chunk creation delegated to RAN Controller.
    - Radio chunk stored in SM.
  - (5GCN/Cloud/edge) Network Chunks:
    - Retrieve information of pool of addresses per slice.
    - Validation of CN capabilities
    - Network chunks creation delegated to VIMs and 5GCN Controller.
    - Network Chunk stored in SM.
- Management of network slices and radio services: These operational flows focus on the commissioning procedures, as well as on the configuration of the collection of chunks.
  - NSI:
    - Create NSI in terms of reserved infrastructure resources.
    - NSI information is stored in the SM as collection of chunks.
  - RAN Service:
    - Radio service object updated/configured and stored in the SM.
    - Linking radio access nodes, belonging to the slice, with 5G CN deployed if it is required.
- Management of application instance: The main goal is to coordinate the NetApps deployment as VNFs.
  - Vertical Services (NetApps):
    - Instantiation/termination of NetApps services by means of NFVO module.
    - NetApps objects deployed and stored in SM.

4.4.2.2.2 TECHNICAL SPECIFICATIONS

The SM implements the network slicing paradigm at three levels: i) Vertical Service Level, where the SM provides a set of services/applications to be deployed in the slice for any client or third-party actor; ii) Network Slice Level, where the deployment of the required NetApps is specified in terms of network functions (physical or virtual) with associated infrastructure/network resources; and iii) Infrastructure Level, where the coordination of the radio, compute, and network resource virtualization is performed. The associated resource requirements related to the network slices are translated into a group of compute, network, and access/transport chunks.

To coordinate the vertical service level, the SM integrates a set of northbound API controllers that interface its internal business layer to translate the requirements of NetApps services in terms of network and infrastructure resources. On the other hand, the SBI comprises different client modules that allow the communication with the resource managers (RAN/TN/5G CN Controllers and VIMs). Notice that the interfaces described below have been defined based on the needs of the Smart5Grid project.

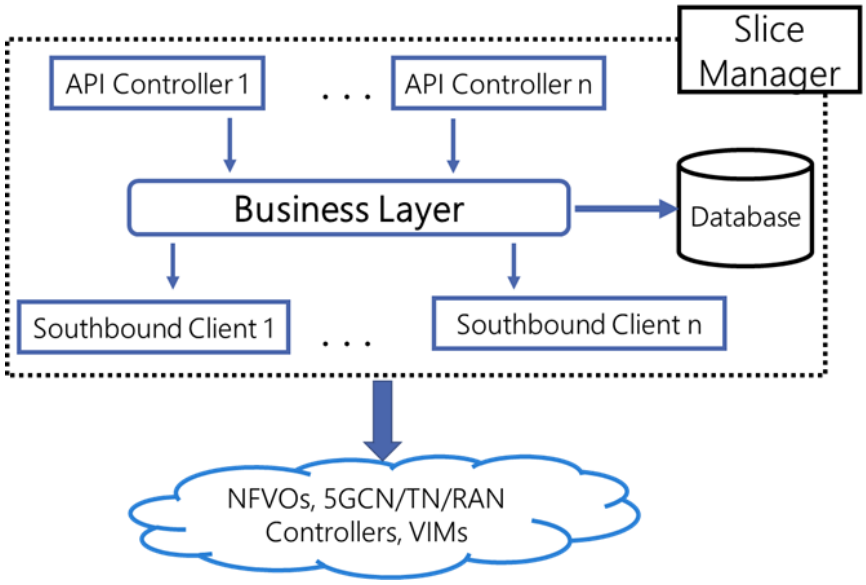

Figure 4-37 Interfaces and relationships of the components from the inside of the SM

In Figure 4-37, the most relevant internal aspects of the SM are defined, while their behaviour principles are detailed below:

- API Controllers: REST-based NBI in charge of:
  - Management of users.
  - Management of infrastructure resources.
  - Management of infrastructure partitions (chunks).
  - Management of NSIs (as collections of chunks).
  - Management of RAN service instances.
  - Management of vertical service instances.

  Each API Controller refers to the type of calls performed by the client or by the third-party actor such as, computing related call, network related call, radio related call, etc.

- Business Layer: It is the key component of the SM which focuses on:

  - Validation of radio topology in terms of interfaces availability.
  - LCM of infrastructure resources in terms of physical hardware model.
  - LCM of infrastructure resources in terms of collection of chunks model per slice.
  - LCM of NSs in terms of instantiation, scaling, and termination procedures for required network functions.
- Southbound Clients: Rest-based interface in charge of:
  - Management of RAN/TN Controller Client.
  - Management of 5G CN Controller Client.
  - Management of VIM Client.
  - Management of NFVO Client.

4.4.2.2.3 INTERFACES AND DATA TO BE EXCHANGED

This section describes a list of the most representative methods implemented by the SM in its NBI and SBI.

Northbound interface (NBI)

Using this interface, SM receives resource reservation and configuration requests from the NetApp Controller for the creation of network slices. In the Smart5Grid architecture, the NBI uses the following methods to implement several REST calls:

- GET {RAN/Compute} Infrastructure: This method provides the information related to the radio devices and compute domains registered previously on the SM. For example, the information exposed by this method can be the location, status, and URL whereby the instances are reachable.
- GET {RAN/Compute} Topology: This method allows gathering information of the RAN and compute resources which can be properly configured and ready to reserve to any other network slice. In other terms, this call allows the NetApp Controller to select the radio and compute resources for the instantiation of a new slice. Notice that this method is purely informative to allow the NetApp Controller to match the resources requested in the NetApp template to the available resources at the infrastructure layer during the instantiation process. The data exchanged by this call includes the name of the radio devices and the cloud domains, their location, their vendor's information and possibly configuration.
- POST {slice_name} Slice: This method allows the NetApp Controller to request a set of radio/compute/network resources for the creation of a new network slice. For example, by using this method in the compute side, the NetApp Controller can provide the IP address by which the VNFs can be reached. Also, the method enables to specify VLAN's information used for the service communication that describes an isolated end-to-end slice. On the other hand, the returned value contains the information of the reserved radio/compute/network resources or an error message in case that the operation fails.
- DELETE {slice_name} Slice: This method allows to perform the decommissioning procedure over a concrete slice as well as removing the previously reserved infrastructure resources to deactivate the whole service communication associated with the slice. The value returned by this method consists of a confirmation or an error message.

Southbound interface (SBI)

The goal of this interface is enabling the communication with the resource managers registered and managed by the SM. The data exchanged through this interface comprises the validation, reservation, and

configuration of a certain amount of radio, cloud, and network resources provided to a specific slice. The REST-based calls implemented can be defined with the following methods:

1. POST {RAN/Compute/...} Resources Validation: This method focusses on the validation of the infrastructure integrity in terms of requested resources. In other words, through the 5G CN/RAN Controllers and VIMs, SM checks the availability of resources to be assigned to a certain slice. The value returned by this method consists of a confirmation or an error message.
2. POST {RAN/Compute/...} Slice Chunk Creation: If the previous verification is correct, the method allows to proceed with the reservation and registration procedures of the specified RAN and Compute resources required by a slice. The method returns a value that consists of a confirmation or an error message.
3. POST {RAN/Compute} Slice Chunk Activation: Once the RAN and compute resources have been reserved and stored on the SM, this method enables to request the radio components and cloud domains activation to start the network service deployment provided by the NetApp Controller. The method returns an information related to the pointed radio/compute resources, or an error message.

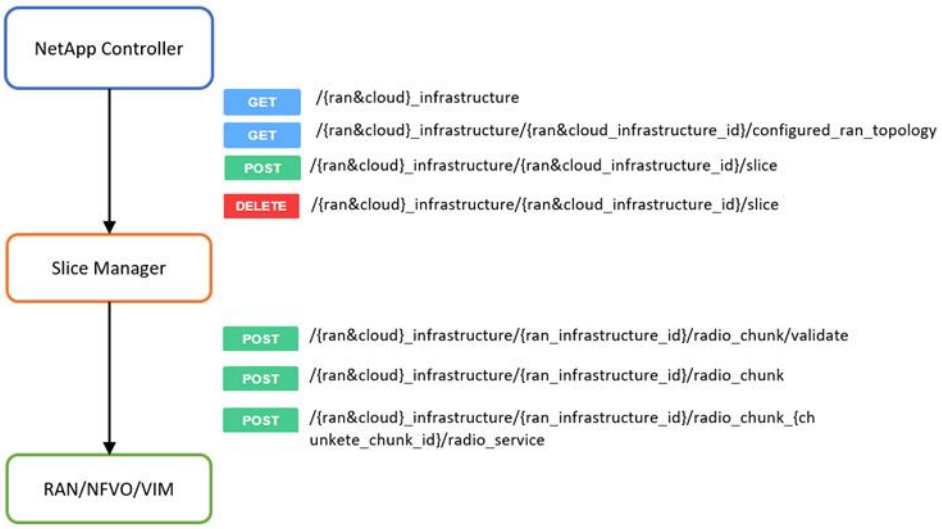

Figure 4-38 Example of interfaces and relationships of the SM with other Smart5Grid components

Data Exchanged during the NetApp Deployment

NetApp Controller is the key element in charge of the whole NetApp LCM, from placement to termination on compute nodes. In that case, NetApp Controller interacts with the SM with the aim to pass a dedicated NetApp descriptor information with specific service requirements. Therefore, NetApp Controller shall exchange data related to the NetApp descriptors and make some REST-based API calls to start the operational flows regarded to the management and infrastructure reservation.

In this context, Figure 4-39 illustrates an example of the interactions conducted during the NetApp service deployment at management and orchestration level. First, NetApp Controller requests the network slice instantiation to the SM (step 1). Following, the SM validates and reserves the infrastructure/network resources by communicating with the resource controllers (step 2). Subsequently, resource controllers configure and register the collection of infrastructure/networks chunks to fulfil the NetApps requirements and then assign them a slice identifier that will be stored within the SM database (step 2.1). After that, the

SM proceeds to add the VIMs chunks in each NFVO involved in the service instantiation (step 2.2). With this information, and once the slice has been created (step 3), the NetApp Controller starts the service deployment procedure where radio and 5G-CN services are configured in order to ensure the end-to-end service communication (step 4). Depending on the NetApp service requirements and the VNFs that it is constituted, NetApp Controller can instantiate NetApps directly by using MEC-host or through the NFVO. In the former case, the NetApp Controller deploys container-based VNFs by interacting directly with the MEC-Host (step 5). In the latter case, the NetApp Controller passes descriptor identifier information (e.g.: ETSI NSD/VNFD/MEC-AppD) to the NFVO. Then, NFVO takes care of the placement and deployment of NetApps over the cloud servers (step 6). Note, it is also possible for a NFVO deploying container-based VNFs at the edge side when using container-based clusters managers as VIMs.

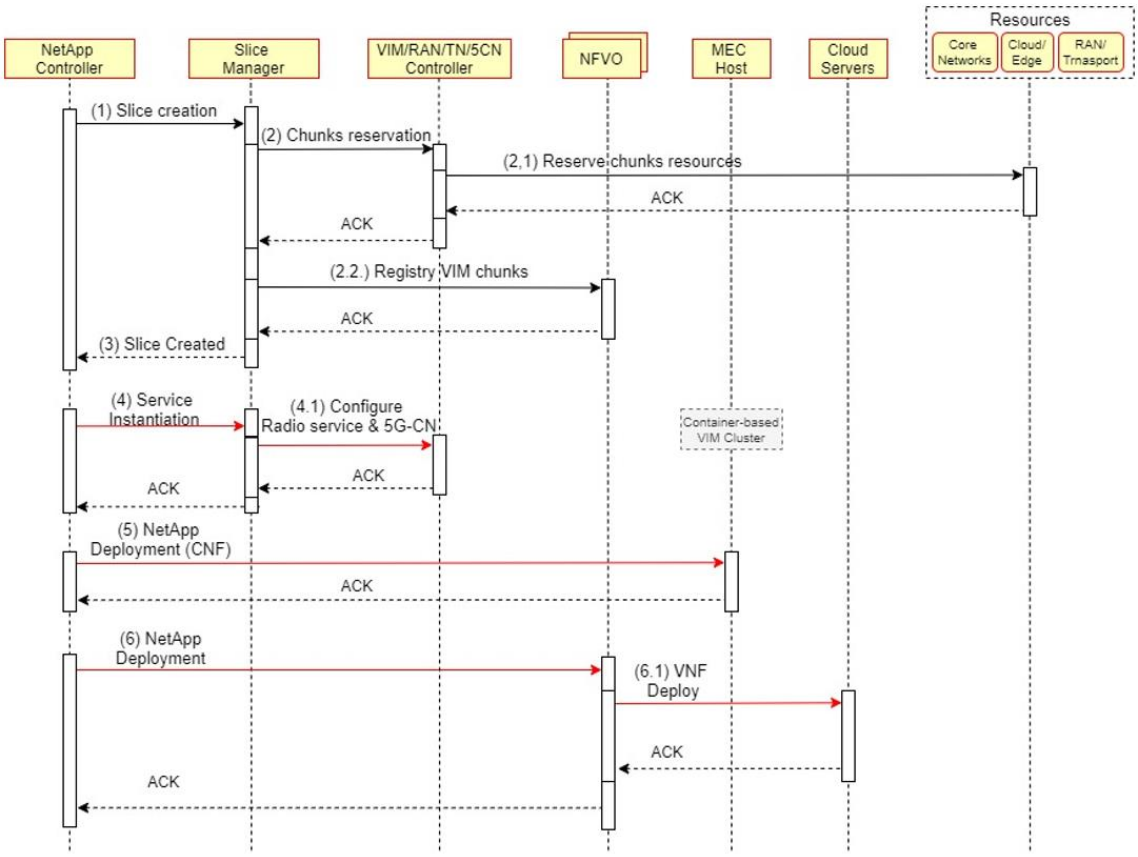

Figure 4-39 Workflow example of the slice instantiation and NetApps deployment over edge and clouds NFVI domains

4.4.2.2.4 SECURITY

Since the SM is not the first point of contact for the customers in the Smart5Grid architecture, it does not implement security methods within its internal modules. However, it is expected that the interaction of the SM with the NetApp Controller and the resource managers will be given in a secure network, where the other Smart5Grid architectural components are running as well. In addition, the SM southbound client entities use security credentials for the interaction with VIMs, NFVOs, RAN and 5G CN Controllers to avoid unexpected access.

4.4.2.3 NFV Framework

In Smart5Grid, to manage VNFs and NetApps, it is necessary to focus on two components of the NFV framework. The first component, NFVO, being the main component of this framework, is in charge of the orchestration of the compute, storage and network resources that are provided by the second component of this framework, the VIM.

4.4.2.3.1 FUNCTIONAL DESCRIPTION

NFVO is a functional block which has one set of functions, Resource Orchestration (RO) and Network Service Orchestration (NSO). The main objectives of the NFVO are the following [61]:

- NS LCM based on VNFM and fulfilling NSO functions.
- Management and orchestration of the NFVI resources of each of the VIMs by fulfilling the RO functions.

Resource orchestrator (RO): The NFVO makes use of RO functions to ensure that resources such as computing and storage resources are available and to allow access to these NFVI resources independently of the VIM to provide the necessary NSs. The RO enables the NFVO to acquire capabilities such as:

- VNFs can collect information on NFVI resources used and their status.
- VNFs can manage the relationship between VNFs and the resources that have been allocated from the NFVI through the information of each VIM.
- Management and use of resource allocation and access control policies for each NFVI.

Network Services Orchestrator (NSO): The NFVO uses the NSO functions. These depend on the exposed services of VNFM and the RO. The capabilities provided by NSO to NFVO are the following:

- Grouping and organizing of associated VNFs in NSs.
- Instantiation of the NSs and configuration of the related VNFs as a whole, configuring the corresponding connections.
- LCM of the instantiated NSs, such as scaling and monitoring.
- Enables policies for managing instances of NSs and VNFs.
- Management of automation of actions scheduled on a specific NS.

4.4.2.3.2 TECHNICAL SPECIFICATIONS

This section details two main topics related to the NFVO, the lifecycle manager and monitoring.

Lifecycle Manager

The lifecycle manager in an NFVO refers to the LCM of the NS, which in turn is responsible for invoking the LCM of the VNFs that belong to the same NS (i.e., the lifecycle operations of an NS are related to the lifecycle operations of its VNFs) The LCM and operations of a NS can be divided into five stages, which are described below [80]:

- NSD is created following the standard, in which the primitives and lifecycle are configured, as well as the grouping of the VNFs and the necessary resources of each one.

- The packets are on-boarded (i.e., injected into the orchestrator so that the defined NS can then be created.) In operations such as onboarding, a series of checks are performed to validate whether there is consistency in the models to be onboarded and the relationships between them.
- NS is created, together with its identifier and related instances of NFs. In this stage, all the processes of instantiation and configuration of each NF related to the NS are carried out, interacting with service platforms such as VIM, and the subscription of the new NS.
- Once the NS is instantiated, automated operations are performed, such as common scaling operations, software update and NS health or actions programmed by primitives in the NS and NFs packages. In addition to the primitives that allow actions to be executed, there are also actions that can be activated internally in the NS and NF packages, such as the monitoring of some parameter of the NFs or the activation of alarms and notifications when a certain threshold is reached.
- The fifth stage is the termination of the NS and its identifier and subscription as well as its related NFs, releasing the resources that had been allocated.

Monitoring

In the world of orchestration, the term metric is well known. This word is defined by the NFV 003 specification [81] as follows: a standard definition of a quantity, produced in an assessment of network performance and/or reliability, that has an intended utility and is carefully specified to convey the exact meaning of a measured value.

These metrics refer to the status of an NS or a VNF and their resources and can be monitored, for which NFVO and other tools come into play to help perform these actions. For these metrics to be monitored, the name of the metric is specified in each VNFD. The monitoring options can be very broad, but the most common is the measurement of the resources of each VNF from the NFVI where it has been deployed. When measuring the metrics, they can be evaluated through the thresholds defined in each VNFD, which will indicate when a scale out/in is needed.

ETSI defines three types of metrics that are obtained from the NFVI where the instantiation takes place [82]:

- Compute Metrics: This generally refers to the CPU. The metrics specified in each VNF will be used to measure and report on the usage of those processors. The VNF instantiation determines which CPU resources to allocate, such as the number of virtual CPUs to use or whether this CPU will be shared with another VNF.
- Network Metrics: Responsible for measuring the traffic load on the different interfaces configured in the VNF.
- Memory Metrics: In charge of measuring the memory usage of the system and its management.

4.4.2.3.3 INTERFACES AND DATA TO BE EXCHANGED

This section describes how NFVO interfaces with SM and NetApp Controller through the NBI, how the SBI works with VIMS and the format of the input descriptors.

Interconnection in the northbound with Slice Manager / NetApp Controller

Northbound interfaces are defined by ETSI in NFV-IFA013 [83]. These interfaces are exposed by the NFVO to the OSS/BSS (Operational Support Systems / Business Support Systems) to perform exchanges over the Os-Ma-nfvo reference point and support the following useful interfaces for Smart5Grid:

1. NSD Management Interface: This interface is responsible for the management of the NSD and performs operations such as: create NSD Info, Upload NSD, delete NSD, among others.
2. NS LCM Interface: Makes possible the invocation of operations from the OSS/BSS NS LCM towards the NFVO such as: NS instantiation, NS scaling or NS termination among others.
3. NS Performance Management: This interface is used to provide information on NSD performance, such as measurement results and notifications. These are operations like Create Threshold operation.
4. VNF Package Management: This interface allows you to manage and perform all types of operations with the VNF Packages.

Southbound interface with VIMs

NFVO consumes the APIs of the VIM controllers via the SBI. The exchanges between the NFVO and the VIM are done through the Or-Vi reference point and supports the following interfaces useful for Smart5Grid according to the ETSI definition NFV-IFA005 [84]:

- Software Interface Management: This interface allows the management of software images in a VIM.
- Virtualized Compute, Network and Storage Interfaces: These interfaces allow the NFVO to perform operations on the virtualized computing resources available on the VIM, such as allocating network, CPU, or storage resources.
- Virtualized Resources Performance Management Interface: This interface provides information about the performance of virtualized resources such as memory over-utilization or disk latency.

Format of the input descriptors

In Smart5grid, when referring to NFV Descriptor, NSD and VNFD are referred to and are modelled using the YANG models of the NFV-SOL 006 specification [85].

According to the NFV-IFA 014 specification [86], the NSD is a template which contains the information used by the NFVO to manage the NS lifecycle. An NS is composed of a set of VNFs with unspecified connectivity between them. As for the VNFD, according to the NFV-IFA 011 specification [87], it is a template that describes the VNF deployment requirements, such as the virtualized resources, interfaces or the OS container image to be used.

In the NSD, the inputs that are generally found, are interconnection inputs, either interconnection inputs from VNFs through Virtual Links Descriptors (VLDs) or interconnection inputs between different NSs or different External Endpoints and Access Points through Service Access Points (SAPs).

In VNFDs, one can find more or less entries depending on the desired requirements of each VNF. The most common entries that are specified can be the CPs, the interfaces, the monitoring and scaling parameters or the definition of the virtualized resources CPU, RAM, and storage, but the most important entry in Smart5Grid VNFDs is the image, which in Smart5Grid is an OS container image.

To manage and orchestrate OS containers, two functions are required, Container Infrastructure Service Management (CISM), in charge of maintaining the workload of the Managed Container Infrastructure Container Objects (MCIO); and Container Image Registry (CIR), in charge of storing the software images of the OS containers. In the VNFDs, the OS container image will be referenced, and the characteristics of its infrastructure resources are collected in attributes in the VDU and in the Connection Point Descriptor (CPD).

The OS Container Image also refers to the declarative descriptor of the container Managed Container Infrastructure Object (MCIO). This descriptor is collected by one or more Managed Container Infrastructure Object Package (MCIOP), which are packages that collect the declarative descriptors of the container as well as the configuration files, which can be referenced with an identifier in the VNFD. All this information, both the VNFD and the packages related to the container to create a containerized VNF, is collected in the VNF Package, as can be seen in the following image of the NFV-IFA 040 specification [88]:

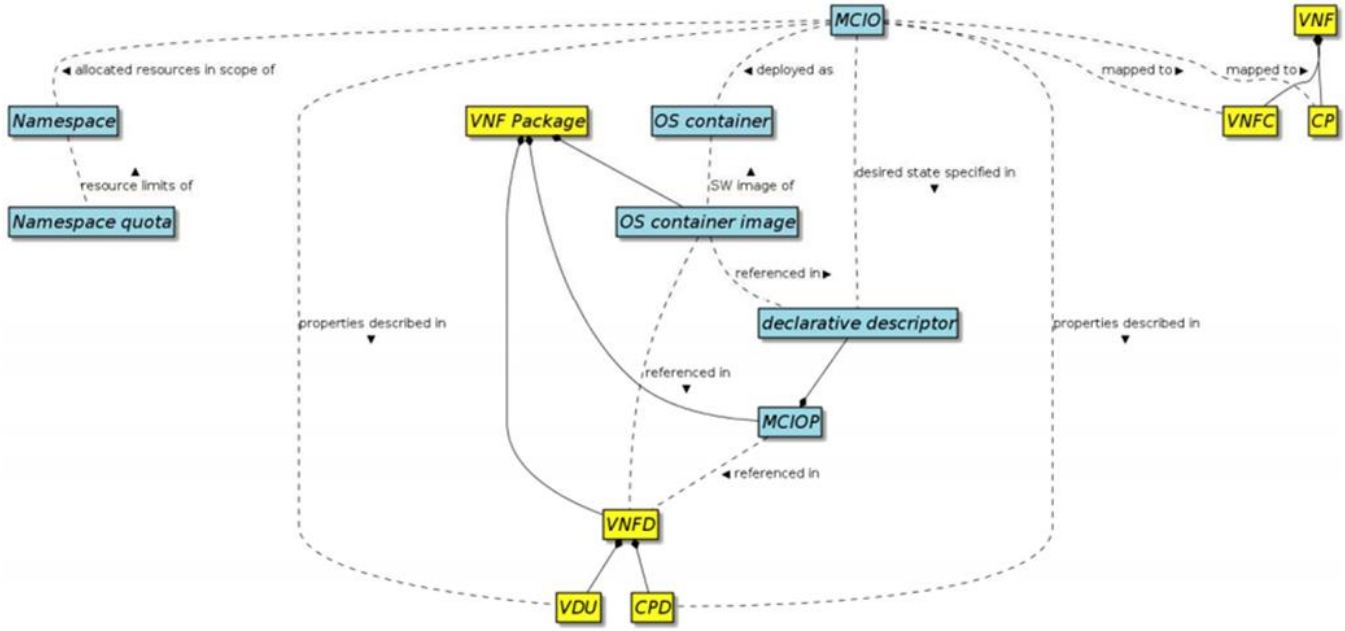

Figure 4-40 Relationship between OS container image and VNFD [88]

4.4.2.3.4 SECURITY

NFVO and VIM are two of the three components of the MANO system, which is defined as a closed system. In the NFV-SEC 014 specification [89], a security analysis is performed in which it is determined that there are threats that can put the system at risk, while there are others found as malware that are not specific to this system but to any network software-based system. Several requirements for maintaining the security of these two MANO components are listed below:

- NFVO does not allow any action before identifying, verifying the identity and location of the transmitting party.
- NFVO provides a closed-loop message and session integrity service.

- Data transferred through the NFVO's internal interface is protected from disclosure to unauthorized entities (i.e.: it provides confidentiality for internal transfers through the use of a network protocol encryption mode).
- NFVO has access control, allowing geographic restrictions for data processing, thus complying with legal obligations and policies.
- VIM has its own security groups configured by default, blocking all incoming traffic to the instantiated VNF, thus preventing it from being accessed. If you have access to this VIM and want to access the instance, you will need to modify this security group or create a new one to allow TCP (Transmission Control Protocol) port 22 access to this VNF via SSH.

4.4.2.3.5 NFVO TO BE USED IN THE PROJECT

Smart5Grid will make use of different NFVOs, due to the design and characteristics of each of the testbed of this project, as well as the different partners that are involved in it. This does not rule out the rest of NFVOs, in fact they could be used if the testbed design requires it.

Open-Source MANO (OSM)

OSM is an NFVO aligned with the ETSI NFV information models. OSM enables the creation of real NSs in production environments. The orchestrator can interact with infrastructure components such as NFVI and VIM. OSM is infrastructure-agnostic (i.e.: the same NSs can be deployed on the different supported VIM types without the need to modify anything in the descriptors).

OSM normally works also as a SM. However, it offers the possibility that the work of the SM can be carried out by an external autonomous system that manages the lifecycle of the slices, while OSM will work as an NFVO making use of the SOL005 interface without the need to augment it [80].

OSM NBI, which is a RESTful API, makes a set of calls to the ETSI NFVO SOL005 API, as it is aligned with the standard. In terms of consuming APIs from VIMs through the SBI by developing a Plugin based on the standard specifications, it allows interoperating with a large number of VIMs without the need for each of them to conform to the standard [90].

As for the OSM Information Model (IM), it has undergone many changes throughout its development, trying to be as aligned as possible with ETSI, so, since version 9, the IM is fully aligned with ETSI NFV SOL006. In addition, OSM has improved the YANG models of the standard by adding, among other things, the support of new VNF and VDU metrics, configurable through yaml files within the VNF package.

NearbyComputing's NearbyOne

NearbyComputing's NearbyOne [91] is an end-to-end orchestrator that covers the role of a NetApp Controller and MECO but also of a NVFO. Since these two roles are complementary and entangled together, it is natural to extend a NetApp Controller and MECO to not only manage the lifecycle of NetApps, but to also govern the lifecycle of all the VNFs that compose the NetApp. Besides, since these two roles are blended, NearbyOne offers a single pane of glass to operate both roles.

4.4.2.4 5G CN Controller

The 5G CN Controller is responsible of the management and orchestration of the resources of the CN. It tightly collaborates with the SM, and, in certain deployments, it can be de facto realized as a submodule of the SM itself. As further detailed in the following, the 5G CN Controller implements some functional capabilities that 3GPP has assigned to NSSMF and the Network Function Management Function (NFMF) [48].

4.4.2.4.1 FUNCTIONAL DESCRIPTION

The 5G CN Controller manages the resources of the 5G CN Slice Subnet. It acts upon request of the SM, which requests CN resources to be reserved and assigned to a specific slice. It is also responsible of the application-level management of the CM, FM, and PM of VNFs, CNFs and PNFs included in the CN slices. In particular, it has full visibility and control over such resources, allocated/deployed in each of the existing CN Slice Subnet Instances, including both cloud and edge network functions. It handles the orchestration (instantiation, LCM, provisioning, service chaining, scaling) of the CN VNFs via direct control over the corresponding NFVO. It also provides the SM with information about the availability of CN resources for the instantiation of new slice instances, and it guarantees a detailed view of the CN resources assigned to each managed slice.

In organizing and handling CN Slice Subnets, the 5G CN Controller also determines what VNFs are shared and what are reserved to specific services. It translates the core domain-specific intent of a service instantiation request into appropriate configurations of the core VNFs.

In other words, the 5G CN Controller needs to support workflows for all the operations of slice LCM, and it needs to translate the calls issued by the SM for this purpose to a series of calls towards the CN resources. More precisely, the lifecycle operations that the 5G CN Controller needs to support at the level of the CN Network Slice Subnet Instances (NSSIs) shall be, as a minimum:

- Slice Modelling and preparation; the 5G CN Controller shall have a series of slice templates that the user shall be able to use.
- On-demand slice creation and instantiation.
- Slice activation.
- Slice monitoring and assurance.
- Slice deactivation.
- Migration of the CN subnet slice components on different resources.
- In service operations, such as:
    - Scale up/down.
    - Scale in/out.
    - Healing.
- Slice termination.

Upon a NetApp deployment, the 5G CN Controller is in charge of finding a good placement for every and each of the core VNFs that are part of the NetApp itself. A good placement means that:

- The NetApp is able to start its execution.
- The resources required by the core VNFs of the NetApp (e.g., number of CPU cores, amount of DRAM, accelerators, etc.) are guaranteed.

- The required traffic steering rules are set in place.
- Upon a failed deployment, the 5G CN Controller should gracefully mark the deployed service as failed and trigger alarms to notify the associated SM (and/or the NetApp Controller via the SM) with the failed deployment.
- Upon a failed deployment, the 5G CN Controller shall undo all the operations performed between the start of the workflow and the failed call, in order to leave the CN Slice Subnet in the same status it was before the start of the workflow.

In case the relocation of a CN resource is requested by the SM (or by the NetApp Controller via the SM), the 5G CN Controller must either execute this relocation or send back a request denial.

4.4.2.4.2 TECHNICAL SPECIFICATIONS DESCRIPTION

As we mentioned above, the functionalities of the 5G CN Controller can be substantially identified with those of 3GPP's NSSMF (intended as a CN domain-specific function) and NFMF. In particular:

- The NSSMF is responsible of the management and orchestration of NSSIs; NSSMF receives NF requirements from NSSI requirements and delegates the management of NFs to the NFMF.
- The NFMF manages VNFs in order to guarantee performance, configuration, and fault management; it interacts with the VNFM to enable the common management of deployed VNFs.

Figure 4-41 depicts how such functionalities are interfaced with the other architectural elements of the NFV MANO layer:

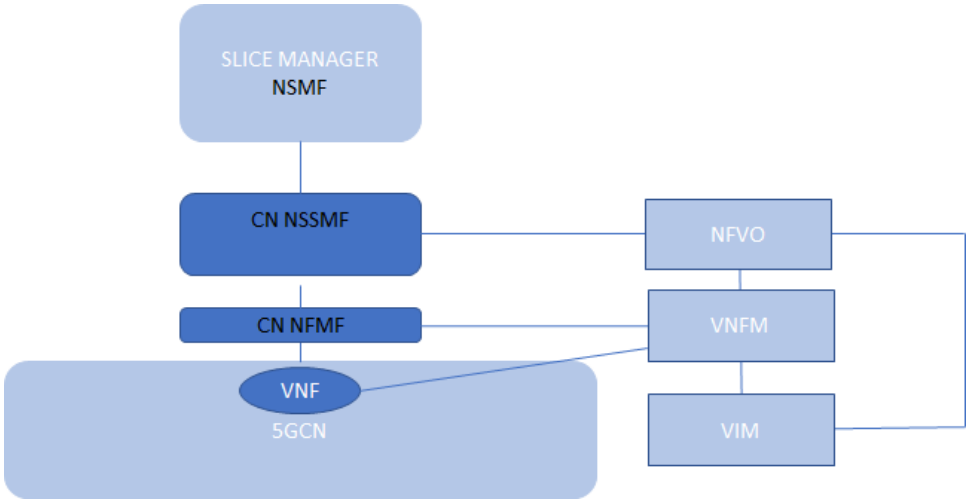

Figure 4-41 Connection between NSSMF and NFMF with the other architectural elements of the NFV MANO layer

4.4.2.4.3 INTERFACES AND DATA TO BE EXCHANGED

For the purposes described so far, the 5G CN Controller exposes a northbound RESTful API towards the SM and a southbound API towards the CN resources (the corresponding NFVO). In particular, the northbound API enables the SM to request the management of CN NSSIs and the reservation of CN resources. The 5G CN Controller supports the protocols used for the configuration and management of the core resources (VNFs, PNFs and CNFs) on the southbound API. The data exchange technologies

supported by the 5G CN Controller are compatible with those of the modules connected to it, to guarantee an appropriate interaction among them and a successful deployment and execution of the NetApps and the other networking services over the network. These technologies must follow the defined standards, in order to let the 5G CN Controller be vendor agnostic in terms of the CN NSSIs it manages.

Finally, the 5G CN Controller is capable of extracting telemetry data from the CN and to expose them (e.g., using Prometheus and Grafana) and make them available to the Telemetry Module (cf. Section 4.5.2.6 Telemetry).

4.4.2.4.4 SECURITY

Access to the 5G CN controller will be allowed via authenticated logins only to the Operations staff in charge of managing the network element. Concretely, in Smart5Grid implementations, access will be permitted exclusively to the personnel of the partners that provide the telecommunication architecture.

Control Traffic and Management Traffic will be transported in dedicated networks (DCN: Data Communication Network), whereas data traffic will be transported on IP network, so that a high level of security is guaranteed; control and management traffic will not have any contact with public network.

4.4.2.5 RAN Controller

The management and configuration of radio devices of the 5G network is handled by a dedicated management module called RAN Controller. This module, which, depending on its implementation, might be a standalone component or integrated with the SM, exposes the available radio infrastructure to the upper layers of the architecture via its Northbound API and enables its configuration and management. The RAN devices of the network are managed over the southbound API of the RAN controller, using dedicated protocols. In the following subsections, the detailed description of the RAN controller module, which forms part of the Smart5Grid architecture, is presented.

4.4.2.5.1 FUNCTIONAL DESCRIPTION

The RAN controller provides the necessary abstraction to the SM to be able to configure and manage the 5G RAN devices of an infrastructure and, as such, it plays the role of one of the core modules of the Smart5Grid architecture. The RAN controller interfaces on one hand with the SM and on the other hand with the radio devices deployed in the 5G network. The 5G NR devices of a deployment are registered in the RAN controller as endpoints; the RAN controller as such is aware of all the radio devices and has an internal representation of the RAN.

First, over the RAN controller's Northbound RESTful API, the RAN controller exposes calls that allow for the configuration of radio devices (physical parameters, logical parameters) to the SM and for polling information about the RAN. During the initial (day 0) configuration of the network, the SM will use the RAN controller to set up the devices according to the desired settings, which are the physical settings, such as operation frequencies, transmission power, radio bandwidth, etc. During the network operation, the RAN controller will allow for the logical configuration of the devices, provide status reports of RAN devices to the SM, and can also expose information to the telemetry system.

Second, the RAN controller integrates with the underlying radio technologies. For this purpose, it implements a southbound API towards the radio devices, using whichever protocols are implemented by

them. The protocols used vary with the RAN device type, but commonly used protocols are NETCONF or SNMP. In some cases, a radio device vendor might also implement its own commercial management system that sits on top of the radio HW. In such a case, the RAN controller integrates with the management system of the vendor, rather than communicating directly with the radio devices. Independently from that, the RAN controller must implement a device discovery method, to be able to understand the RAN topology, and to expose this information to the SM. Similarly, the RAN controller must expose status information to the RAN hardware to the SM, e.g., by continuously polling the status of each radio element and exposing this information.

4.4.2.5.2 TECHNICAL SPECIFICATIONS

In the following subsections, the technical specifications of the RAN controller are given, focussing on the aspects that are relevant for the Smart5Grid deployment.

RAN Device Manager

The core of the RAN controller is its device manager, a subsystem that has full awareness and control of the RAN devices deployed in an infrastructure. The registration process of RAN devices, which can be proactive or reactive depending on the implementation on the radio device, is the first step necessary to enable device management. Once registered, the device manager module has access to the configuration calls of the radio devices and can poll information from the devices. The device manager can then expose this information to the upper layers, i.e., it enables a third element (like the SM) to request the configuration of the devices for both physical and logical parameters. All the status information of the devices is stored locally in the RAN controller, on a dedicated database. It is important to note that RAN controllers might support different radio technologies, like 4G, 5G or Wi-Fi. Each technology has its own representation in the database, but also its specific data model.

Device Abstraction Layer

Each RAN controller of a deployment or UC may support specific 5G NR RAN vendors. To support a variety of vendors, but also different radio technologies, ideally a RAN controller implements a device abstraction layer. This abstraction layer introduces transparency to the device management module, by converting generic calls into the specific call required by a particular RAN device.

In Smart5Grid, each UC deploys a RAN network based on one or several commercial solutions. In some deployments, like UC2, there is also the potential support for other technologies, like legacy Wi-Fi via the RAN controller. The capability of abstracting the different technologies and vendors in a UC deployment and to integrate them all within a single RAN controller and even interconnecting the technologies is a feature that can substantially increase the flexibility and the connectivity options for a deployment.

Radio Telemetry

RAN statistics can be key to understanding the performance of a UC. During operation of the network, 5G radio nodes may collect a series of statistics and metrics about the connectivity towards the UEs like aggregate throughput in up and downlink, the resource block assignments, the channel quality for particular bearers, etc. These statistics can be stored and shared with the telemetry module and reviewed

using dedicated tools, e.g.: Prometheus. With tools like Grafana [92], they can be visualized, or they can be exposed to other services that analyse the RAN performance.

4.4.2.5.3 INTERFACES AND DATA TO BE EXCHANGED

The RAN controller features northbound and southbound APIs to communicate with the SM module and the radio devices, respectively. This subsection briefly describes the key interactions executed over these APIs.

Northbound API: Towards the Slice Manager

The NB API exposes calls towards the SM that allow to configure the radio infrastructure, choose a part (or all) of these radio elements to form part of a new RAN chunk, i.e.: a subset of the available RAN resources, and to configure it to form a logical, isolated slice that is connected to the UC services. The northbound API is REST-based.

Southbound API: Towards the radio devices/radio management system

Any interaction with the RAN devices, i.e.: the 5G NR small or macro cells, including the configuration of physical and operational parameters of the RAN devices, is handled over the southbound API of the RAN controller. Protocols used in these interactions include NETCONF and SNMP, but they are specific to the hardware vendor. Alternatively, to talking directly to the RAN devices, a vendor might expose its own radio management system that uses e.g.: a REST-based API.

4.4.2.5.4 SECURITY

Security is another important aspect of the RAN controller design. Like other components of the architecture, the access to the RAN controller and in particular its endpoints need to be secure, i.e., no unauthorized access can be allowed. Also, it is expected that access and configuration of the RAN devices is only possible through a specific access methodology.

The access to the RAN controller will only be given to other endpoints within the same network, i.e., the network in which the SM and the RAN devices are deployed. This connectivity can also be enabled over a VPN. Further, for interactions between the radio devices and the RAN controller, credentials or security keys are used to assure that no unwanted access is possible.

4.4.2.6 Telemetry

The network/IT infrastructure monitoring is handled by means of the telemetry component that is the main ingredient able to inform any optimization engine or planning tool on how to place VNFs and NetApps closer to the device or migrated to a more powerful cloud environment if needed. Often, this choice or the potential system configurations are unknown to application developers ahead of time. What might be the right choice for a low-end device (such as a smart meter) with good connectivity may be a wrong choice for a high-end mobile device (drone). So, the Smart5Grid platform will collect and manage the different data coming from processing and networking infrastructure in a smart way.

Summarizing, the telemetry component main functionalities can be restricted to the following list:

- To collect and store measurements related to the resource utilization of the NFV, NetApp and underlying VIMs. More generally speaking, the telemetry module, when data are available, can collect information at any level of the entire stack that comprises the network slice (from RAN to CN).
- To homogenize these measurements and metrics using a common data model irrespectively of the employed NFV/VIM technology and make them available to all services that need them to coordinate their performance profiles.

4.4.2.6.1 FUNCTIONAL DESCRIPTION

The telemetry component introduces different internal services with distinct corresponding roles and responsibilities. Specifically:

- The monitoring service (M) collects metrics from different computing and NS.
- The translation service (T) transforms and enriches the collected metrics by incorporating information from the M&O environment.

These two functionalities serve any kind of execution engine in Smart5Grid that is responsible to communicate concrete recommendations and the configuration directives to the Service Orchestrator of the NFVO.

4.4.2.6.2 TECHNICAL SPECIFICATIONS

More specifically, all the running services of Smart5Grid exchange messages carrying various types of data through a brokering mechanism. The responsibility of the monitoring service is to collect data from different types/technologies of NFVIs, as well the application domain, and assess critical KPIs about the performance of the running application services and the status of the network.

This information is later used by other services of the Smart5Grid infrastructure. Specifically, monitoring services expected to collect data from the following sources so depending on the sources (OpenStack-based cloud computing environments, Kubernetes management platforms, etc.) or from the M&O domain (i.e.: NetApp Controller, 5G CN controller, RAN controller). For each integrated environment, special data adaptation module will be introduced to homogenise metrics from the corresponding environment to the Smart5Grid ecosystem.

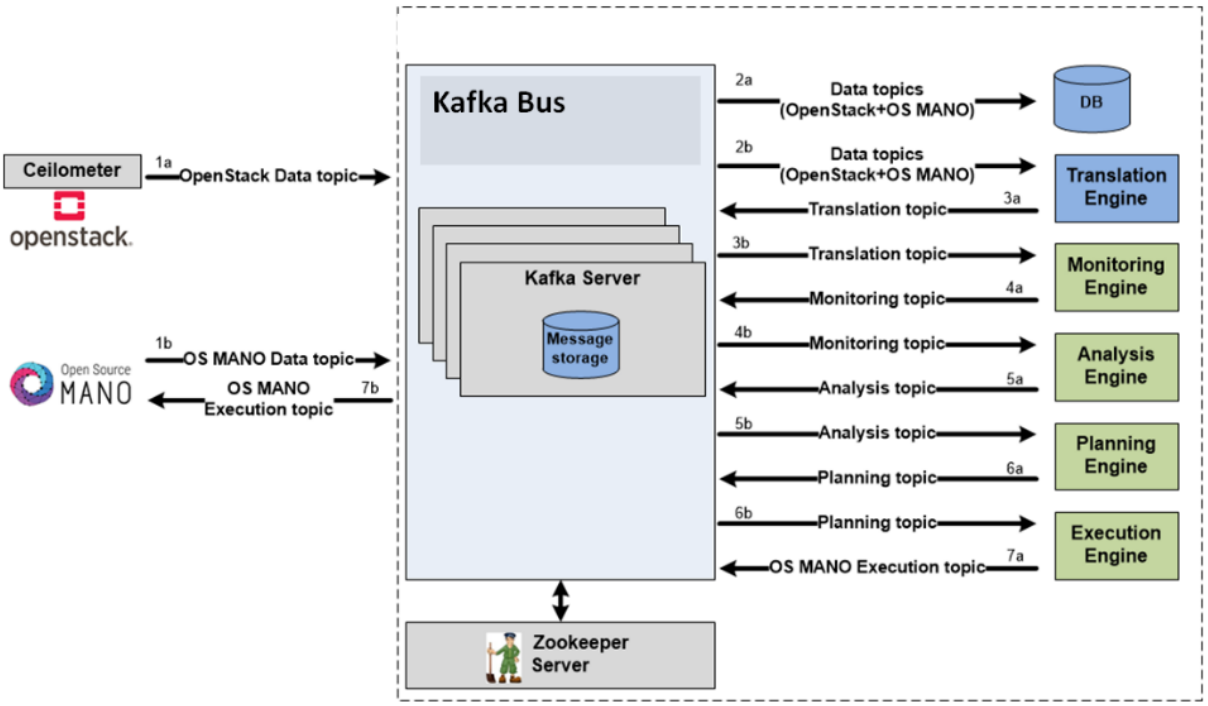

Figure 4-42 PSB Functionalities

As an example, Figure 4-42 illustrates a solution in which a broker mechanism based on Apache Kafka [93] interacts with an OSM instantiation and an OpenStack VIM, working in synergy with the general functions that can in a general way be put in place and are represented in boxes.

In this representation, the telemetry will rely upon the broker to collect and spread information for allowing the various engines to exchange messages with each other, as well as to receive/send information from/to external systems. This is based on Apache Kafka processing software platform, which enables the efficient handling of asynchronous events and notifications.

The interaction between monitoring and OpenStack is related to the collection of performance and status metrics, enabled by the use of Ceilometer telemetry tool, which is a service that meters the performance and the utilization of OpenStack resources. However, any other meter from other open-source product can be used. It can itself send events to a storage service or, in case of samples, they are sent to a service named Gnocchi [94], which is optimized to handle large amount of time-series data.

In general, this tool provides support for:

- Collecting metering data in terms of CPU and network costs.
- Collecting data by monitoring notifications sent from services or by polling the infrastructure.
- Configuring the type of collected data to meet various operating requirements.
- Accessing and inserting the metering data through the REST API.
- Expanding the framework to collect custom usage data by additional plugins.
- Producing signed and non-reputable metering messages.

But any other monitoring metrics can be handled and from different open-source projects as Open nebula.

4.4.2.6.3 INTERFACES AND DATA TO BE EXCHANGED

The telemetry block broker interacts with different services and, with the normal development of the project, new services can be added and normally managed. Here, we a have a first list that leaves a degree of freedom on the open cloud infrastructure choice. For the sake of clarity, a general indication on OpenStack and K8s is provided.

The monitoring part can have different interfaces depending on the type of messages exchanged. For example:

- It receives a set of monitoring data from the open-source cloud infrastructure publisher and publishes them in a dedicated topic in the publish/subscribe broker.
- It processes the incoming raw monitoring data from the NFVIs, VNFs and network elements, adapts them in a common data model and correlates each metric with a running network service.
- It stores all the required OSM information per VDU (VM or container) that is needed from the translator service to run.
- It imports the monitoring data in the database after the adaptation process completion.

4.4.2.6.4 SECURITY

The security will be based providing at minimum the following functionalities:

- In-flight encryption of data using SSL/TLS.
- Authentication using SSL.
- Authorization using Role Based Access.

These main properties can be modified, or new ones can be provided after the analysis of UCs data.

4.4.3 Open-source cloud infrastructure software selection

As regards the open-source cloud infrastructure software, different solutions are analysed that will be the base for the final specifications. The final decision will be based on the requirements of the UCs and the necessary extensions, if needed, will be designed to adapt the platform to the host infrastructure.

OpenStack

OpenStack [17] is an open-source project facilitating companies the creation of their own cloud computing setup. It creates an Infrastructure as a Service (IaaS). OpenStack lets users deploy VMs and other instances that handle different tasks for managing a cloud environment on the fly. For more details about the 5G and Energy development over a cloud infrastructure and the enabling related technologies, you can refer to [95] and [96].

Inside the OpenStack environment, there are different packages and components. The main components are:

- Compute: Open-source software designed to provision and manage large networks of VMs, creating a redundant and scalable cloud computing platform.
- Object Storage: Open-source software for creating redundant, scalable object storage using clusters of standardized servers to store petabytes of accessible data (code-named "Swift").

- Image Service: It provides discovery, registration, and delivery services for virtual disk images (code-named "Glance").

There are also other projects and services that make up OpenStack, some of them are:

- Horizon [97]: The project that provides the graphical dashboard that allows for the management of the cloud compute resources through a virtual interface instantiation management that is an OpenStack environment itself.
- Nova [98]: To manage computer resources.
- Neutron [99]: A network module which is responsible for taking control of the network translation from the IP addresses of the host operating system and the IP addresses that are associated with the VMs.
- Keystone [100]: OpenStack service providing identification and authentication of API clients to ensure that the system itself is locked down.
- Heat [101]: OpenStack project dedicated to orchestration.

CloudStack

CloudStack [102] is based on the management server and the related resources to be managed. The management server is the CloudStack software that manages the cloud resources and allocates resources in the cloud deployment. It provides a web interface for administrators and end users, as well as API interfaces.

The management server also manages the assignment of guest VMs, the assignment of IP addresses, allocates storage during VM instantiation, and manages snapshots, disk images, and ISO images. It is a single point of configuration for the IaaS cloud and during deployment the user informs it of the resources to be managed.

The CloudStack deployment is organized with hosts contained within clusters, clusters contained within pods, pods contained within zones, and zone contained within regions. Regions are the largest available units in the CloudStack deployment.

Interesting development of SDN controller and smart grid relying on 5G infrastructure can be find in [103] with the direct involvement of CloudStack.

OpenNebula

OpenNebula [104] was initially released in 2008 and now operates as an open-source project. Whereas it is mostly used for private cloud, it also supports public and hybrid clouds.

The OpenNebula architecture is a classical cluster with a front-end and a set of cluster nodes to run the VMs. The architecture is flexible and modular, making it easier to integrate multiple storages, network infrastructures, and hypervisor technologies. The OpenNebula software consists of three layers:

i) The Tools layer provides interfaces to communicate with users and allows users to manage VMs through the interfaces, which include CLI and libvirt API [105]. This layer also contains a scheduler that manages the functionality of the core layer.

ii) The Drivers layer contains components that communicate directly with the underlying operating system and capture the underlying infrastructure as an abstract.

iii) The Core layer contains the components used to perform user requests and control resources. In this layer, disk images for VMs are stored using datastores (referred to as Image Repositories in previous releases). The monitoring subsystem gathers information on the hosts and the VMs, such as basic performance indicators and capacity consumption, and it also contains the authentication system, which comes with a built-in user/password authentication driver and the choice from SSH Authentication, X509 Authentication[28], and LDAP Authentication[29] also. The latest OpenNebula version, equips OpenNebula with a new provisioning tool so that cloud admins can now expand their private clouds in an incredibly flexible way, using resources offered by third-party cloud providers incorporating, when necessary, distributed dedicated infrastructure. OpenNebula users can automatically allocate resources when needed, deploying, and controlling edge nodes based on the current demand at those specific geographical locations. This approach significantly simplifies the process of provisioning and managing edge resources, without the organization that is using this solution having to provide or own those underlying resources at all. As regards 5G, the combination of AWS and OpenNebula's First 5G Edge Architecture based on AWS Wavelength [106] enables true hybrid and edge cloud computing by combining public and private cloud operations with workload portability and unified management of any infrastructure and applications.

Cloud Native ecosystem

With recent advances within in containerization and effort from manufacturers, Cloud-native VNFs may now run in a container rather than a Virtual Machine, their lifecycle orchestrated by a container orchestration engine such as Kubernetes (https://kubernetes.io/), and their observability enhanced by advanced monitoring tools (Prometheus).

With regards to the Cloud Native VNF design, the following projects are relevant:

• Ligato [107] is a Golang framework intended for development of custom management/control plane agents for cloud native VNFs. The framework includes a set of specific functionalities: logging, health checks, messaging, REST and gRPC (Google Remote Procedure Calls) APIs. Ligato is part of the "Runtime - CloudNative Network" CNCF category.

[28] In cryptography, X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key. Also see, among others: https://en.wikipedia.org/wiki/X.509

[29] LDAP is a lightweight version of the Directory Access Protocol (DAP). Its original goal was to provide low-overhead access to an X.500 Directory, but the tool now has a wider variety of uses. LDAP's primary function is enabling users to find data about organizations, persons, and more. It accomplishes this goal by storing data in the LDAP directory and authenticating users to access the directory. It also provides the communication language that applications require to send and receive information from directory services. Also see, among others: https://sensu.io/blog/what-is-ldap

• Gohan [108] is an industry open-source project that proposes schema-driven micro-services development framework

4.5 Energy infrastructure involved in the pre-piloting

This section will review the energy infrastructure to be involved in the pre-piloting phase as well as in some demonstration sites of the Smart5Grid project. Specifically, it will provide:

(1) A functional description of the power equipment or other type of monitoring sensors to be installed in a dedicated section of the power grid, within the scope of two out of the four Smart5Grid UCs (demonstrators);
(2) Their technical specifications, with a focus on the communication aspects;
(3) The needed interfaces and type of data to be exchanged with the Smart5Grid platform. Where relevant, security aspects will be also detailed.

Power systems are highly critical infrastructures. Therefore, before testing any new equipment or sub-system solutions that might affect the actual operation environment of a portion or up to the entire grid, it is mandatory that these solutions are thoroughly tested and validated in a controlled operation environment such as a digital twin, Real-Time Hardware In the Loop (RT-HIL), testbed infrastructure, etc. This is known as pre-piloting testing and validation stage. As such, this chapter will first detail the architecture and equipment involved in the HIL tests related to the specific UCs of the Smart5Grid. Functional description, technical specifications, and interfaces with real power equipment to be involved in two of the demonstrators will be also detailed.

4.5.1 Real-Time Hardware In the Loop testing environment

The Power System Testbed (PST) of KIOS CoE, University of Cyprus (UCY), will be used as a pre-piloting testing facility in two out of the four demonstrators of the Smart5Grid. The testbed offers a versatile testing and validation environment from modelling, simulation, emulation, and experimental validation of energy systems, with capabilities from developing smart converters for the integration of RES and storage technologies to wide area monitoring and control of smart power grids. Further, the PST might be used to develop, validate, and demonstrate intelligent management and control schemes, or embedded control algorithms for smart grids under realistic operation conditions.

The testbed supports open-source standards, and the communication with the testbed is based on industrial common protocols in order to avoid vendor lock-in situations.

4.5.1.1 Architecture

The general architecture of the PST is briefly presented in Figure 4-43. It is to be noted that the PST of UCY has a flexible design which allows several re-configurations able to investigate different kinds of scenarios specific to the Smart5Grid UCs. This general architecture of the testbed is composed of three main architectural blocks, and only part or all of them might be required, depending on the UC and the specific operation scenario to be tested and validated. In the following, the role of each of these components, and how the Smart5Grid platform will be integrated in this set-up is briefly described.

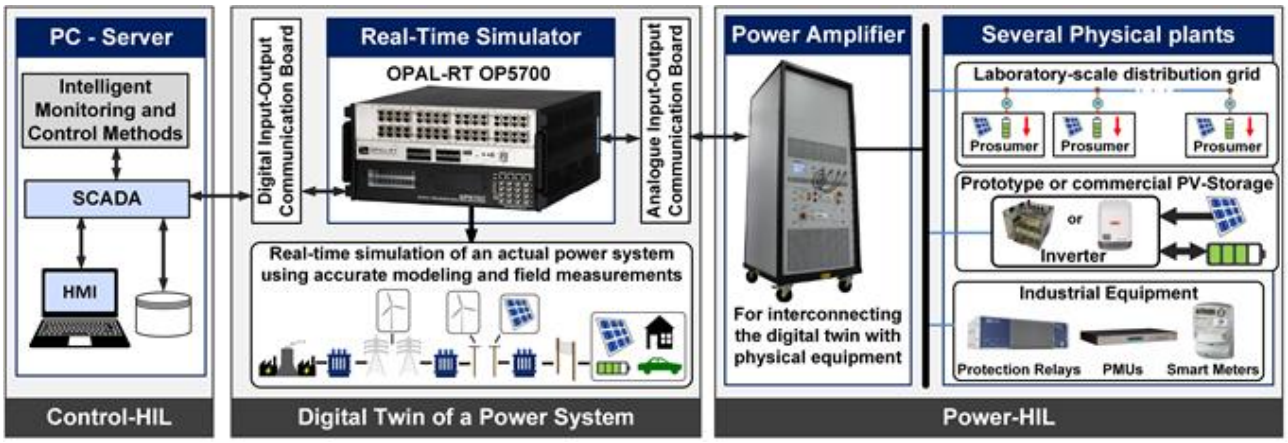

Figure 4-43 General architecture of the power system testbed

1. Digital twin implementation of a power system: The role of this block is to develop and implement accurate power systems models in the real-time simulator making use of field measurements and parameters of the actual power grid or section of the power grid that it mirrors.
2. Control-Hardware In the Loop (Control-HIL): The role of this block is to offer a development framework where detailed models of the power system (or small-scale prototype plat) under test is included in the loop with the developed controller.
3. Power-Hardware In the Loop (Power-HIL): The role of this architectural block is to offer a framework to investigate the interaction between the digital twin of a power system and the physical plants (i.e., prototype or commercial inverters of PV or of a wind turbine, and/or of a Battery Storage System (BSS), industrial equipment used in power grids such as protection relays, smart meters, PMUs, etc.).

Within the scope of the Smart5Grid, the PST of UCY will be complemented with a hardware network emulator (hardware and software unit) aiming to emulate the 5G data communication stream between the actual field sensors or measurement units to the Smart5Grid platform, while the Smart5Grid platform will be integrated in the Control-HIL of the PST, as it can be seen in Figure 4-44.

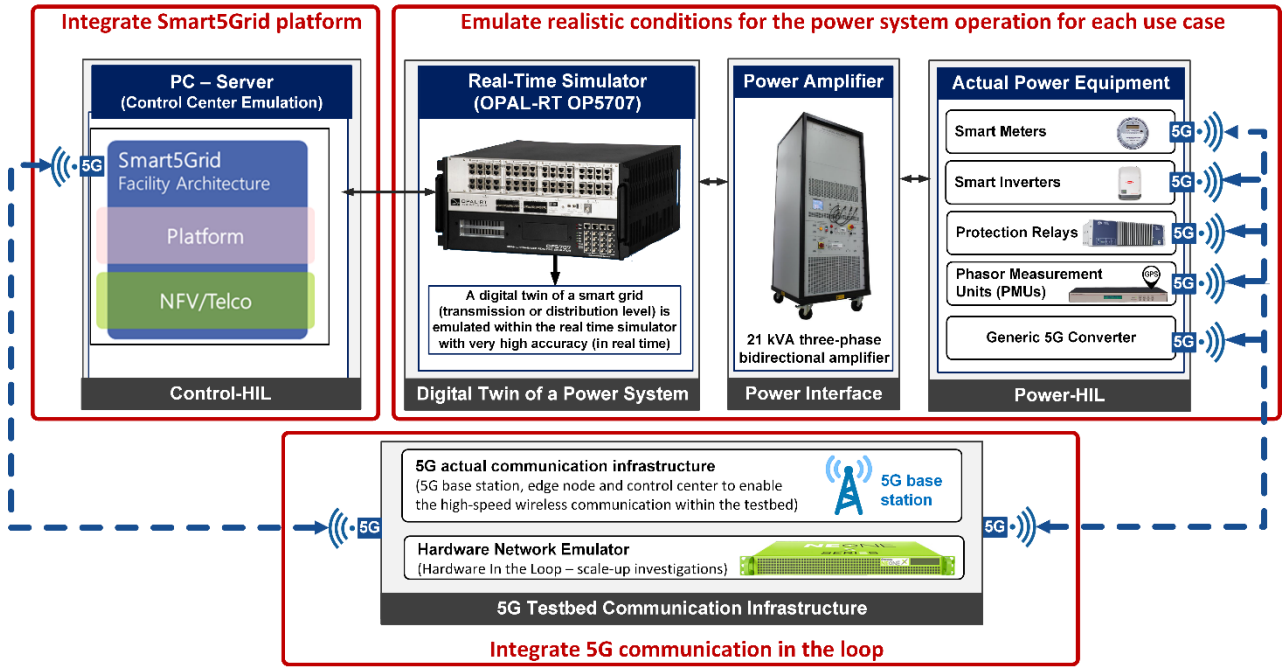

Figure 4-44 Smart5Grid HIL architecture for pre-piloting tests

4.5.1.2 Functional description

The different functional entities that form the HIL architecture for pre-piloting tests are described below:

Control-HIL

The Control-HIL is a framework where the Smart5Grid platform along with the developed controllers are included in the loop with the digital twin power system implemented in the real-time simulator. It is to be noted that the Smart5Grid platform will be the middleware between the NetApps and the PST.

To consider the complexity of the power system in real time, either a small-scale prototype plant or the digital twin of the actual power plant can be used. Thus, the controller is able to receive measurements and send control set-points to the power grid under test (digital twin), emulating realistic conditions for the demonstration. In actual systems and in control-HIL framework, the real-time responsiveness of the controller is crucial for the stability of the whole system besides any communication or processing delays.

Digital twin of a power system

The implementation of a digital twin of a power system is crucial for creating realistic conditions to test and validate the specific UC NetApps, which in turn aim to provide additional services for the grid and to enable the power systems' evolution. A dedicated Real-Time Simulator (RTS) is required for the development of a digital twin of a power system. Thus, a computational powerful RTS (OPAL-RT OP5700 [109]) is used to allow the execution of high-accuracy simulations in real time. Field measurements (collected from actual power plants either online or through measurement campaigns) are employed in these simulations to replicate the operation of selected power systems as digital twins. As a result, a digital twin of an actual power system allows the execution of studies and investigations for evolving the operation of a smart grid without risking the integrity of the infrastructure.

Power interface

For the investigation of the interaction between the power grid under test (digital twin) and a market available or a prototype plant to be integrated in the smart grid (e.g., aiming for new or more advanced functionalities or services), a power interface is used. In this context, the power equipment is interconnected with a selected bus within the digital twin through a power amplifier. The power amplifier replicates, in every solution step of the digital twin (every 50 μs), the voltage conditions of the selected bus, and this voltage supplies the power equipment. The operation of the power equipment (power exchange with the amplifier) is considered by the digital twin to accurately emulate the interaction between the two.

Power-HIL

Power-HIL framework investigates the interaction between the power grid under test (digital twin) and a physical power equipment in the loop. This allows the testing of how a prototype or a commercial equipment will operate when it will be connected to a specific location within an actual power system. Therefore, the dynamics of the power systems are replicated in a realistic way to investigate the operation of a physical equipment under a relevant environment. Examples of physical power equipment are PV plants, BSS, the electrical installation of a building, Wind-Turbines, devices used by power industry (i.e., smart meters, PMUs, protection relays, etc.), laboratory-scale distribution grids, etc. On the other hand,

power-HIL is crucial to validate and demonstrate how a new power equipment will properly operate when it is connected to an actual power plant. For the latter case (e.g., development of prototype power equipment such as wind power inverters or new protection system for the power grid, etc.), the power-HIL infrastructure can be used for validating the operation of the prototype equipment under extreme scenarios and under realistic conditions.

Hardware network emulator

A similar concept as the digital twin for the power grid could be obtained for the 5G network using the hardware network emulator component of the HIL-Architecture. This is in principle a software-defined test network which mimics the effects of real-world networks, including 5G technology. The NE-ONE Model 10 Network Emulator from ITrinegy [110], with 2 x emulation ports, 10 links and scenario builder function is used. The NE-ONE allows to create accurate, controllable, and repeatable network conditions such as latency and jitter, re-ordered or duplicated data packets, lost/corrupt data or queued and congestion conditions among others. The network emulator also allows for emulating network tests from simple network types such as point-to-point, multi-link, and dual hop up to highly sophisticated network types such as fully or partially meshed, star-coupled, chained-hop networks.

4.5.1.3 Interfaces and data to be exchanged

As part of the HIL tests, several physical equipment from the power HIL architectural block will be involved, such as: smart meters, smart inverters (for PV or battery storage units), PMUs and protection relays. The interface between the physical power equipment (e.g., sensors or measurement units, smart inverters, or protection relays) and the HIL digital twin is realized by a power amplifier, whereas no interface is needed between the HIL and the network emulator.

Each type of power equipment might be subject to a specific communication protocol. In what concerns the power equipment to be involved in the HIL pre-piloting phase, three types of communication protocols will be involved, namely the MODBUS TCP/IP [111], IEEE C37.118 Communication Protocol [112], and the IEC 61850 series [113].

Smart meter measurements need to be collected through MODBUS TCP/IP [111] protocol within a LAN to monitor the generation of individual RES within a RES park. Similarly, control commands can be sent to RES inverters to coordinate their operation through Modbus protocol. This will allow the active management of RES park. This HIL framework may be related to the UC3 of the Smart5Grid project.

Measurements taken from PMUs installed in digital substations are collected through IEEE C37.118 Communication Protocol [112], and they are reported to a Phasor Data Concentrator (PDC) located in the control centre to enable wide area monitoring and control applications for smart grids. This HIL framework is related to the UC4 of the Smart5Grid project.

Protections relays within a digital substation are receiving measurements from analogue voltage transformers (VTs) or current transformers (CTs) or from digital merging units (through IEC 61850 [113]-Sampled Value (SV) protocol). The measurement is processed to detect grid faults and trip breakers to protect the grid or the substation. IEC 61850-Goose messages [113] for blocking or tripping can be sent to other relays within the same substation or nearby substations to improve the protection scheme behaviour.

Furthermore, IEC 61850-MMS [113] can be used for receiving some measurements or for modifying the protection scheme parameters. This HIL framework is related to the UC1 of the Smart5Grid project.

4.5.1.4 Security

All the power equipment involved in the HIL pre-piloting uses private data communication. In the case of smart meters and smart inverters, a Local Area Network (LAN) or Virtual Private Network LAN (VPN-LAN) will be used. In the case of PMUs, a dedicated private wide area network will be used (private WAN). For the protection relays a private LAN or VPN-Lan will be used.

4.6 Smart5Grid NetApp Descriptor

In order to describe the interactions among the NetApp components presented in Section 3.1, Smart5Grid defines an information model with the aim to capture all the necessary details to completely define a NetApp and its characteristics. This definition is registered in a NetApp Descriptor file that can be packaged with the rest of the elements referenced in it (i.e., VNFs), forming a NetApp Package.

This section describes the first version of the Smart5Grid NetApp information model. It is expected that this definition may face changes and adjustments during the life of the project and beyond, to accommodate unforeseen needs that may arise during the development phase of the project, from NetApp developers, consumers, and infrastructure providers.

Figure 4-45 shows a basic representation of the structure of an exemplary NetApp. The NetApp is composed of VNFs that are interconnected in chains and can be grouped together as NSs. These NSs expose SAPs that can be used to connect to the Telecoms network. In the definition of this interconnection, the expected policies for that specific type of traffic and communication needs to be provided, so a Network Slice can be setup to satisfy it. Alternatively, these SAPs can also be used to expose services from the NetApp to external applications or users such as operators, in the form of APIs or dashboards. The NetApp supports the definition of SLOs with requirements over the set of metrics exposed by the VNFs, which can be used by the NetApp controller to trigger scaling or migration actions. By performing these actions, the compliance with said SLOs can be guaranteed.

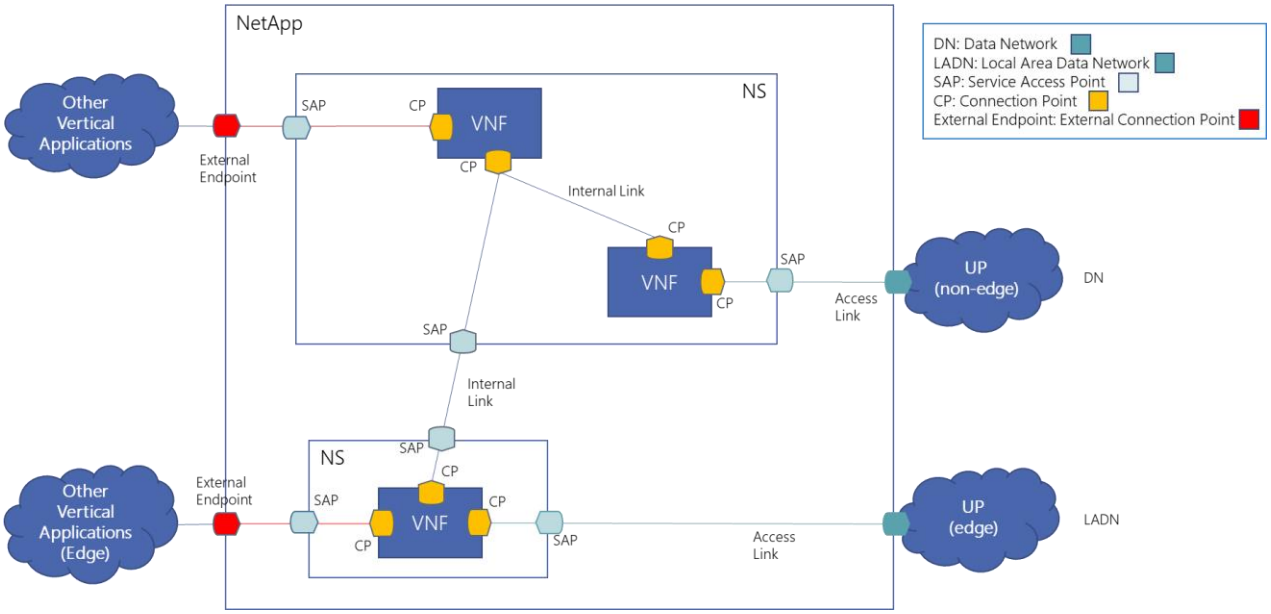

Figure 4-45 Example of a NetApp structure

When defining the information model, it was clear that previous work needed to be continued, and defining new models for network functions forming the NetApp would be undesirable and inadequate in the timeframe in the project. Moreover, the involvement of multiple NFVOs in the project made it difficult to settle on a single existing information model. The aim of the project at the time of mapping the NetApp requirements into an information model was to reuse as much as possible existing definitions and tools. That is why Smart5Grid proposes to adopt ETSI-aligned descriptors and incorporate them into Smart5Grid NetApps in such a way that existing VNFs can be reused. This however may be difficult to bring into reality as multiple implementations in the orchestration layer are available in the different UC implementations within the project, and even ETSI initiatives such as OSM include proprietary definitions of certain aspects, especially in the case of containerized workloads, which are still under specification by ETSI. For this reason, it is proposed to use a hybrid solution where a placeholder for ETSI standard descriptors exists for future implementation, meanwhile allowing existing specific implementations to work in such deployments.

Figure 4-46 represents graphically the Smart5Grid Information Model and its relationship with existing ETSI NFV Information Model.

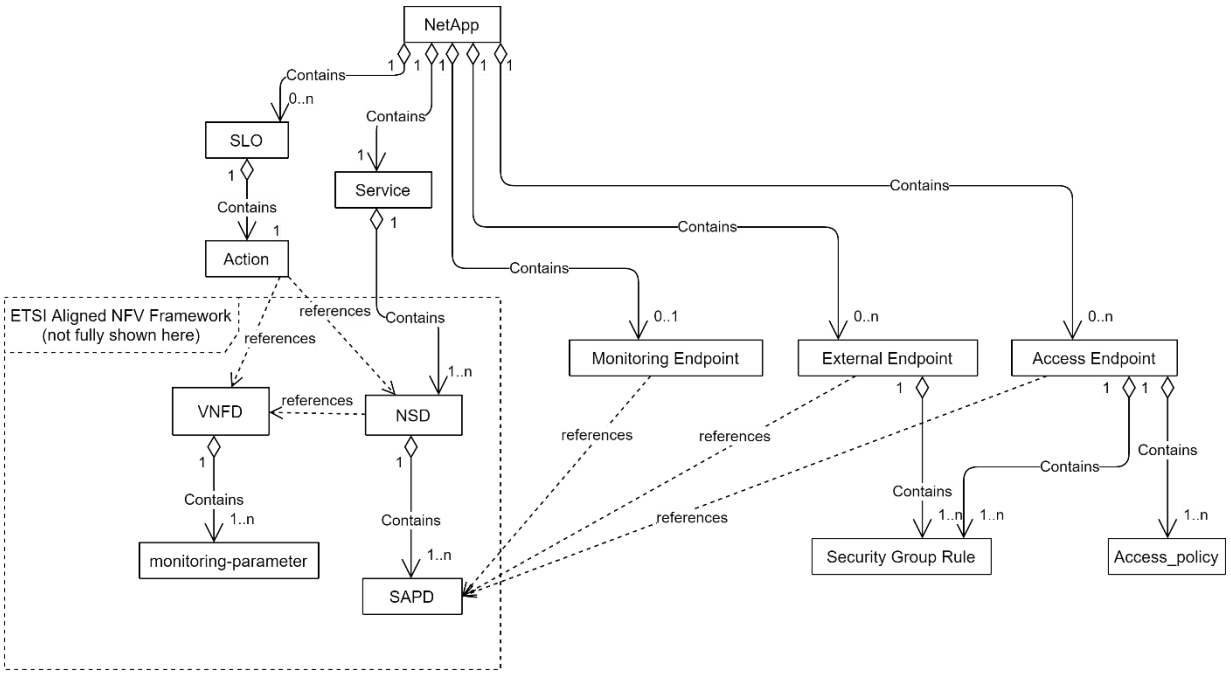

Figure 4-46 NetApp Information Model and relation with ETSI NFV IM

Each of the items in the information model are described in this table:

Item	Type	Content
NetApp	Object	Main NetApp container object
NetApp.Provider	String	Provider of the NetApp
NetApp.Name	String	NetApp Name
NetApp.Version	String	NetApp Version
NetApp.Description	String	Description of the functionality of the NetApp
NetApp.Format	String	Format of the Service item. Allowed values are: • OSM_IM: ETSI OSM Information Model • NBC_IM: Nearby Computing Information Model • ETSI_SOL006 [85] (Placeholder) • ETSI_SOL001 [114] (Placeholder)
NetApp.Service	Object	Service type object. This service is defined in the format specified by NetApp.Format field.
NetApp.Monitoring	Object	Monitoring type object.
NetApp.External	Object	External type object.
NetApp.Access	Object	Access type object.
NetApp.SLOs	List	List of SLO type objects that apply to the NetApp
SLO	Object	Service Level Objective
SLO.name	String	Name of the SLO
SLO.expression	String	Time series data aggregation expression. Either the field metric or expression must exist in an SLO object.

Item	Type	Content
SLO.metric	String	Reference to the metric when presented as already aggregated. Either the field metric or expression exist in an SLO object.
SLO.threshold	Integer	If the value of the SLO is GREATER Than or LOWER than (see "threshold_type" field) this value, it constitutes a violation of the SLO.
SLO.threshold_type	String	Type of the threshold. Allowed values are GT (GREATER THAN) or LT (LOWER THAN)
SLO.Action	Object	Action type object describing the action to be taken if SLO is violated.
SLO.granularity	Integer	Every Number of Seconds that this SLO will be checked. A value of "0" means best effort.
SLO.cycles	Integer	Number of cycles of granularity time that the thresholds must be crossed in order to consider a violation of SLO.
Action	Object	Action container object
Action.target_ref	String	Reference to the target VNF or NS on which to perform an action.
Action.target_df_ref	String	Reference to the target Deployment Flavour for the action.
Action.step	String	Action to be executed every time the SLO is violated. Allowed values are: • TRIGGER_SCALE_UP • TRIGGER_SCALE_IN • TRIGGER_MIGRATION
Monitoring	Object	Monitoring Endpoint container object
Monitoring.sap_ref	String	Reference to the SAP where the NetApp monitoring service is reachable.
Monitoring.url	String	URL where the SLIs exposed by the NetApp are available.
External	Object	External Endpoint container object
External.name	String	Name of the External Endpoint container object
External.sap_ref	String	Reference to the SAP where the NetApp service reachable through this external endpoint is available
External.security_group_rules	List	List of Security_group_rule type objects applicable to the External Endpoint
Access	Object	Access Endpoint container object
Access.name	String	Name of the Access Endpoint container object
Access.sap_ref	String	Reference to the SAP where the NetApp service reachable through this access endpoint is available
Access.security_group_rules	List	List of Security_group_rule type objects applicable to the Access Endpoint
Access.policies	List	List of Access_policy type objects applicable to the Access Endpoint
Access_policy_policy	Object	Access Policy container object

Item	Type	Content
Access_policy.key	String	Name of the specified Access Policy. Allowed values: • Latency: Maximum Latency (ms) • Jitter: Maximum Jitter (ms) • Bandwidth_UE: Minimum Bandwidth per UE (Kbps) • Bandwidth_aggr: Minimum Bandwidth aggregate (kbps) • Availability: Minimum Availability (number of nines) • Reliability: Minimum Reliability (number of nines) • Density: Minimum Device Density (UE/km2)
Access_policy.value	Integer	Value of the specified Access Policy
Security_group_rule	Object	Security Group Rule container object in the format of ETSI Standard descriptor defined in SOL006.
Security_group_rule.id	Integer	Id of the Security Group Rule
Security_group_rule. Description	String	Description of the Security Group Rule
Security_group_rule. Direction	String	Direction of the Security Group Rule. Allowed values: • Ingress • Egress
Security_group_rule.ether_type	String	Type of the Security Group Rule. Allowed values: • IPV4 • IPV6
Security_group_rule.protocol	String	Protocol of the Security Group Rule. Allowed values: • TCP • UDP • Any
Security_group_rule.port_range_min	Integer	Minimum port number of the range applicable to the Security Group Rule.
Security_group_rule.port_range_max	Integer	Maximum port number of the range applicable to the Security Group Rule.

Table 4-1 Smart5Grid NetApp Information Model

5 UC specific NetApps

This section presents an update on current design status of the NetApps identified in D2.1 [1] UC description. Four NetApps have been identified, each serving one of the UCs.

5.1 NetApp UC1

The first UC implements a telecommunications network monitoring mechanism that oversees the status of the local network to improve the remote-control connectivity between the entities that are engaged in the power distribution ecosystem. Although EDI offers an advanced real-time self-healing mechanism, not all primary and second substations are equipped with communication infrastructure to activate the mechanism. In the event of communication problems, the troubleshooting process requires a decent amount of effort and time from the technicians. Since there aren't any related tools that assist in the process, a series of inspections for connectivity checks on the field devices will take place. The 5G infrastructure offers great flexibility in the grid management, offering to the NetApp the necessary combination of availability, reliability, and network latency.

Many of the EDI's primary and secondary substations are connected using either 4G or optical fiber. Through a closed and secure VPN tunnel the network traffic is tunneled to the Supervisory Control And Data Acquisition (SCADA) infrastructure. The 5G connectivity can improve the current communication infrastructure offering a more financially viable solution compared to optical fibre for remote areas and a more reliable solution compared to 4G in case of congestion. The NetApp will monitor in real-time a mirrored version of the network traffic of the field devices and the RAN's overall situation, providing the necessary information (latency, bandwidth, data rate throughput, etc.) to the TLC-Team (TLC, Italian acronym for Tele-Control, one of the main actors of the UC as defined in D2.1).

5.1.1 Architecture

Figure 5-1 presents the vision for the system that will be developed for UC1. The medium voltage (MV) protection devices and RTUs forward the network traffic through an end-to-end tunnel to SCADA. A separate parallel monitoring traffic flow is forwarded towards the deployed 5G infrastructure, then to the Edge Site and eventually to the virtualised function of the NetApp for further analysis and monitoring. The use of the 5G technology enables the reliable monitoring of the network traffic without interrupting the secure communication channel between the field devices and the SCADA or putting at risk the grid. Regarding the communication protocols that are used from the field devices, the MV protection devices use IEC 61850-MMS/GOOSE protocol, while the RTUs utilize IEC61850-MMS/GOOSE/IEC60870-5-104 to forward the collected data. In the case of a detected network issue, the NetApp is responsible to raise an alarm to the TLC Team. The infrastructure's sensors also communicate with ENEL's central SCADA system using the existing optical fibre infrastructure. The two communication streams are independent; the 5G communication infrastructure is used only for monitoring capabilities, while the optical fibre can actively intervene with the deployed sensors.

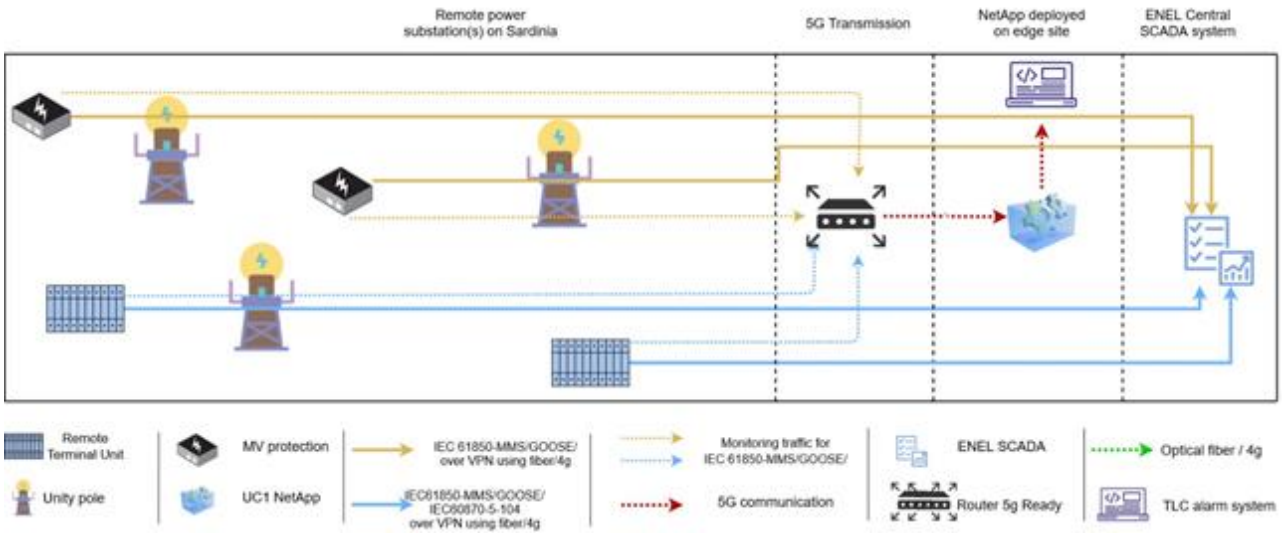

Figure 5-1 UC1 Architecture

5.1.2 Software Components

The infrastructure in UC1 includes a main SW component, the monitoring and fault detection NetApp. It consists of three separate subcomponents: a) receiver subcomponent, b) fault detection subcomponent and c) the monitoring subcomponent

The NetApp receives the network flow via the receiver subcomponent and generates a normalized flow which is forwarded to both monitoring and fault detection subcomponents. The fault detection subcomponent detects any anomalies in the network flow using signature and ML-based techniques and informs the monitoring subcomponent. On top of that, the monitoring subcomponent performs basic flow analysis, logs the related information, and informs the TLC team, via 5G communication, on the network status (both regular and irregular network traffic).

Figure 5-2 illustrates the software component architecture. The information for the status of the network is collected in the deployed sensors via a passive network to the edge in the deployed NetApp using the 5G infrastructure, and eventually the TLC team is informed.

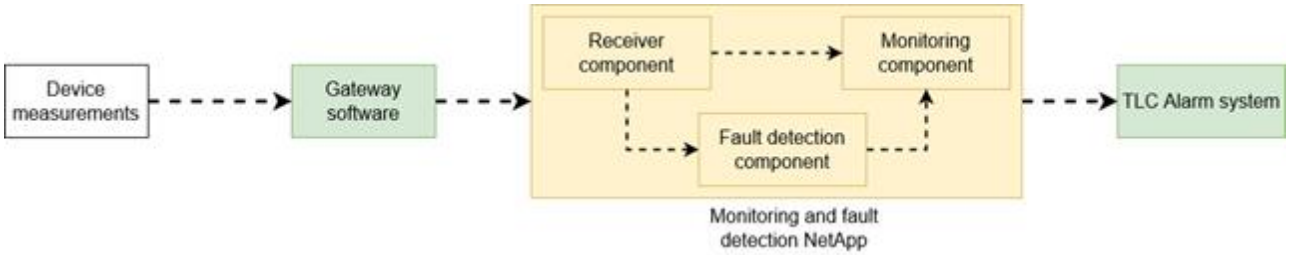

Figure 5-2 UC1 Software Component Architecture

5.1.3 Scenario description

The NetApp that will be developed in the context of UC1 passively receives information from the substation's field devices and delivers the results to the TLC team. Since this section is focused on the development of the NetApps, the interaction with the UC1's actors (TLC team, GDSs – Global Digital

Services – control room, field workforce, TELCO point of contact) is neglected and the focus is given in the exchange of information between software.

Figure 5-3 presents the flow of information between the different software components. The deployed sensors forward the network packets to the receiver subcomponent. The NetApp receiver subcomponent receives the network packets and, upon normalisation processing, forwards network flows into both the NetApp fault detection subcomponent and the NetApp monitoring subcomponent. The former deploys signature-based and ML-based algorithms for detecting anomalies, and the latter constantly monitors the network flows and any potential anomalies and forwards the analysis into the TLC's alarming system. The alarming system is responsible to inform all the engaged actors to operate based on the security plan, while the flow of information is not affected from the findings of the NetApp, as further detailed in the next subsection.

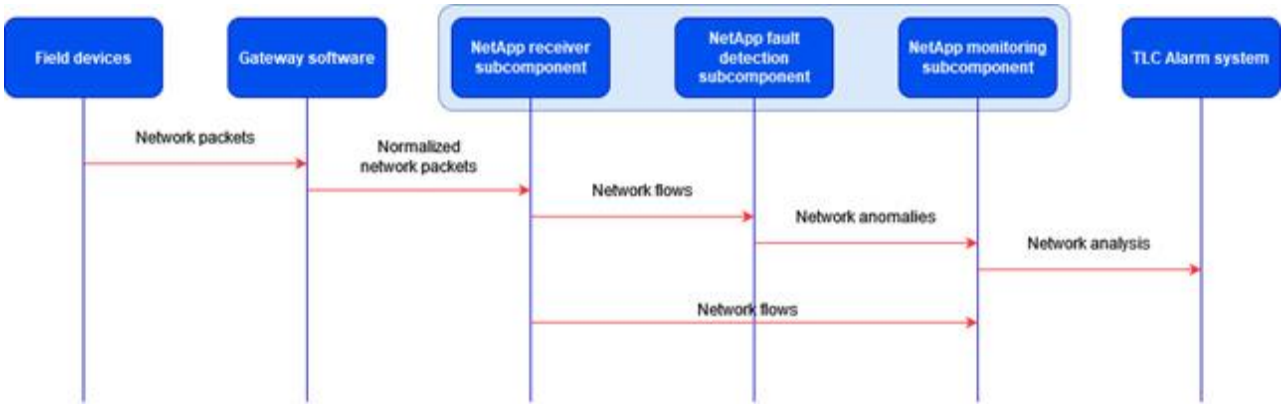

Figure 5-3 Flow of information to the NetApp for UC1

5.1.4 Data flows and management

The target of the NetApp is the analysis of the data traffic quality indicators such as latency, jitter and packet losses from the substation router linked to the field devices. Depending on the quality indicators, different strategies and alarms will be provided. The Figure 5-4 below summarizes the flow of monitoring data between the NetApp and one of the involved substations.

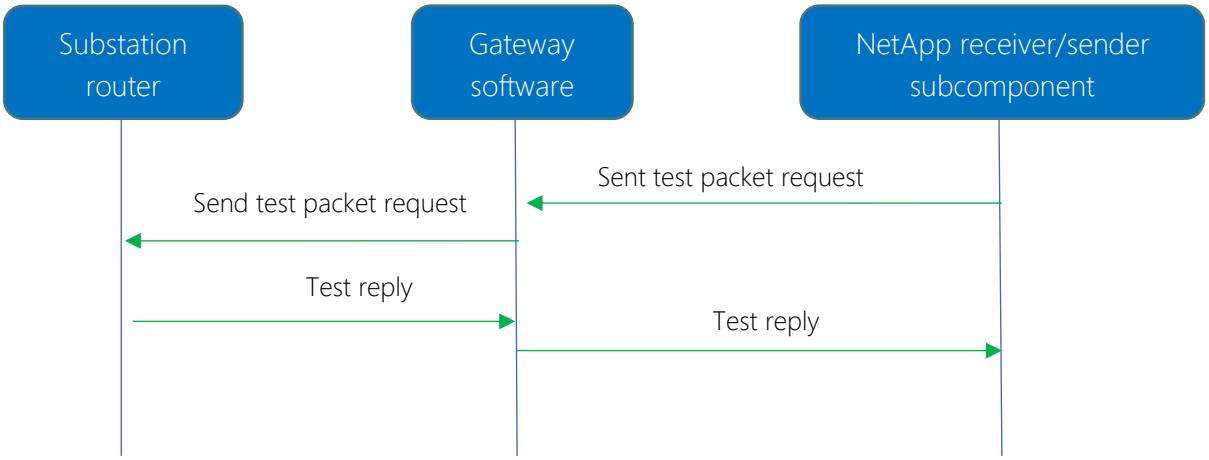

Figure 5-4 Dataflow diagram

Latency and jitter

The test is performed by measuring the time it takes for the substation router to reply to a request from the NetApp. The NetApp sends a message to the server, upon receiving that message, the substation router sends a reply back. The round-trip time is measured is measured in ms (milliseconds). This test is repeated multiple times for a fixed period, and the lowest value determine the result. If the delay is higher than a certain threshold, adjustable as a configuration parameter, an alarm is generated. Similarly, for the jitter, which represent the latency variation.

Packets losses

Packet loss occurs when one or more packets of data traveling across a network fail to reach their destination within the specified time. Services may experience interruptions if packets are frequently lost. If the NetApp fails to receive packets from the substation router for three consecutive intervals, a fault indication is triggered and an alarm signal is generated and reported to the distribution master station. After communication is restored and data is transmitted as normal for more than 40 ms the alarm will be cleared.

Since this is a 5G at edge substation application scenario, the traffic generated by the NetApp against the field devices is monitored for the aforementioned parameters of jitter, latency and packet losses. Those monitoring data, as summarized in Table 5-1, are collected, processed, and analysed locally. Statistical records and eventually alarms can be sent to the regional control room.

Table 5-1 UC1: Monitoring data

Data ID	Data Description	Data Type
Plant ID	A string value containing the substation code	String
timestamp	The timestamp when the detection occurred	Timestamp
latency	Latency time in ms	Float
jitter	Jitter period in ms	Float
PacketLoss	Number of lost packets per second	Float

The monitoring traffic, generated by the NetApp placed inside the Telco network, will be sent only to the 5G network interface of each edge substation router. Each interface is configured to join a dedicated mobile private Access Point Name (APN)[30], accessible only by the NetApp and used for the monitoring purpose only. Such configuration allows to consider the connection among field devices as part of a private network within the operator´s public network, that doesn't have any connection to internet or any other private APNs used for remote control and automation purposes. In addition, no interactions are allowed between routers on the same private APN.

It is important to remark that the substation routers in use are compliant with ENEL cyber security guidelines elaborated in according to international standards like the ISO/IEC 27001:2013 and technical recommendations provided by the NIST (National Institute of Standards and Technology).

All traffic, including the monitoring traffic exchanged between NetApp and the dedicated 5G network interface, is managed with a whitelisting approach and least-privilege approach, in addition any events

[30] APN is defined in 3G-PPP Specification #: 23.003, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729

regarding our equipment is logged and sent to a Security Information and Event Management (SIEM) infrastructure. All our communications devices on field are accessible only from our secured central control room. In this way we can trust that all strictly needed traffic is exchanged and all the users that operate on the infrastructure can perform few activities according to their privileges.

The information collected by the NetApp will be send in a secured channel (potentially trough a VPN tunnel, to be privately agreed among the Wind 3 and the Enel), through the telco infrastructures, to an external point from where only permitted users, such as Enel technical back-office operators, can read or modify this information.

5.2 NetApp UC2

The second UC introduces a mechanism that detects in real time the exposure of workers and their tools when they enter a forbidden area while they work in the EcoGarraf substation. The security of the workers that operate in electrical stations is of major importance for every energy operator, since it is a place of high risk where the voltage is over 66kV. The safety standards will be the highest while constant revisions will take place integrating the latest technological advances. In the context of Smart5Grid, the 5G functionalities through the development of different NetApps will enhance the safety measures and provide a safer working environment.

The current infrastructure uses two different safety systems: the first one is a camera software with an integrated image recognition that provides an overview of the workers that are physically located in the substation; the second system is UWB (Ultra-Wideband) that provides basic location information through tags and anchors. The technological leap on the current infrastructure is to merge data from different sources, process them and implement the communication channels using 5G technology.

5.2.1 Architecture

Figure 5-5 presents the vision for the system that will be developed for the UC2. The UWB unit (tag and anchor) streams the data to the sync switch and then, the data are transferred, via 5G, into the virtualised function of the NetApp. The camera unit (camera device and image processing unit) delivers the output to the NetApp via 5G through an IP68 switch. The synchronization NetApp collects the information from the two sensors, evaluates it, and informs the workers on site if they - or their equipment - have entered a forbidden zone triggering both the vibration mechanism in the UWB tag and the alarm unit.

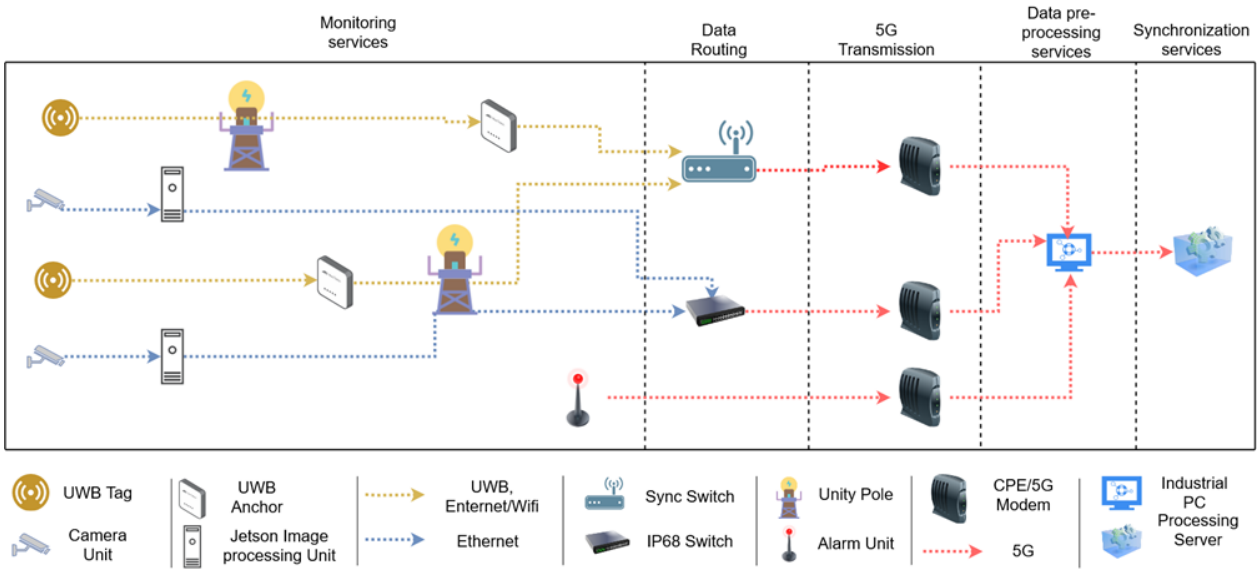

Figure 5-5 UC2 architecture

5.2.2 Software Components

The UC2 architecture includes six SW components, which communicate with each other providing a higher level of safety to the workers compared to the current safety installation. The six SW components are: the front-end application, the Jetson camera software, the UWB software, the Data Synchronization, the KPIs Dashboard, and the area violation component. More specifically:

- The front-end application will be responsible to illustrate the volumetric safety area, allowing the safety manager to define the forbidden zones and monitor the actions in real time.
- The Jetson camera software that accompanies the camera unit. It receives the image from the camera, and it integrates a neural network capable of detecting movement.
- The UWB software collects the information from the deployed sensors. As the workers are moving in space, their action is captured by the sensors, and it is delivered to the Synchro NetApp.
- KPI evaluation and Dashboard will gather the results from the synchronization and calculate / demonstrate the KPIs for the administration.
- The Data Synchronization component will receive and merge the information from the previous components, evaluate and validate them to trigger the alarm system, if necessary.
- Area violation component which will be responsible to trigger the audio and visual alarm hardware.

Figure 5-6 illustrates a high-level architecture of the NetApp in UC2. The figure presents both the input/output and the intercommunication between the aforementioned software components. The front-end application offers an interface to the security personnel to provide the safety coordinates, the cameras' software receives input from the deployed cameras, and the UWB sensor software receives the traffic that is identified from the sensors in the field. Finally, the Synchro NetApp synchronizes the input from the installed software and produces the related information and alarms.

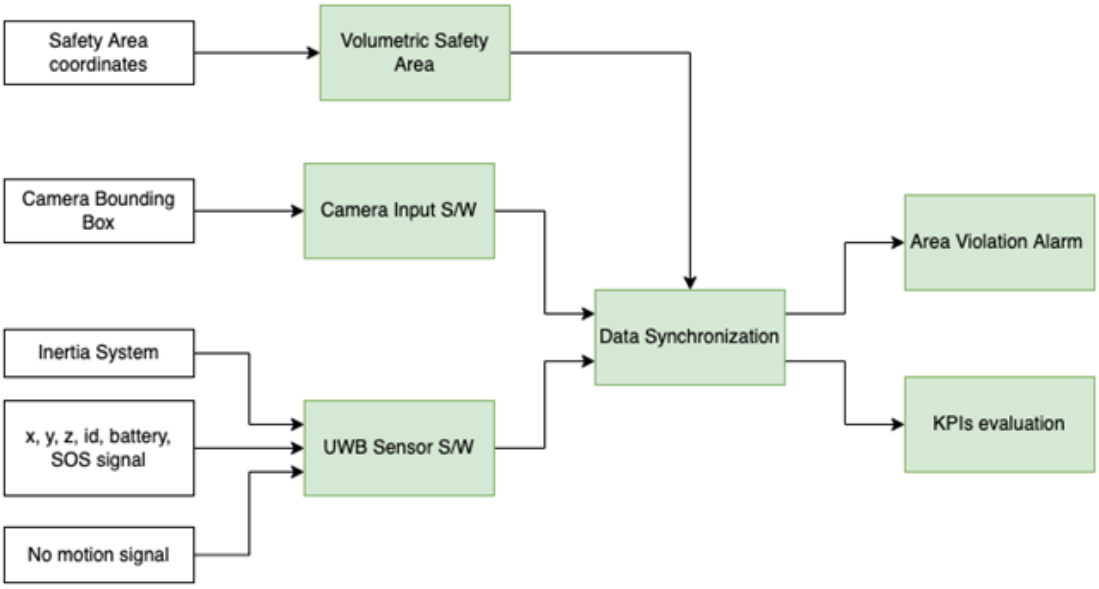

Figure 5-6 NetApp S/W component architecture of UC2

5.2.3 Scenario description

The NetApp that will be developed in the context of UC2 receives information from two different sources, motion sensors and camera, proceeds in processing the receiving information, enables the synchronization mechanism, and informs the security workers if they have entered a forbidden zone. Two scenarios are covered in this UC: in the first scenario, the worker enters the primary substation and stays in the predefined area and no warning is triggered; in the second scenario, the worker cross passes the safety area and triggers the alarm.

Figure 5-2 presents the sequence diagram that covers both scenarios. In the first phase, the motion sensors, that the workers wear on their wrist, and the cameras that are placed to the site, forward the coordinates to the NetApp receiver subcomponent. Then, the input data are transformed into the unified data flow and forwarded to the NetApp computing subcomponent, where the necessary pre-process takes place to normalize the different inputs and export the harmonized data flow which is forwarded into the NetApp synchronization subcomponent. Eventually, the final decision for triggering or not the alarm is taken, and the worker receives the warning if he has entered the forbidden zone.

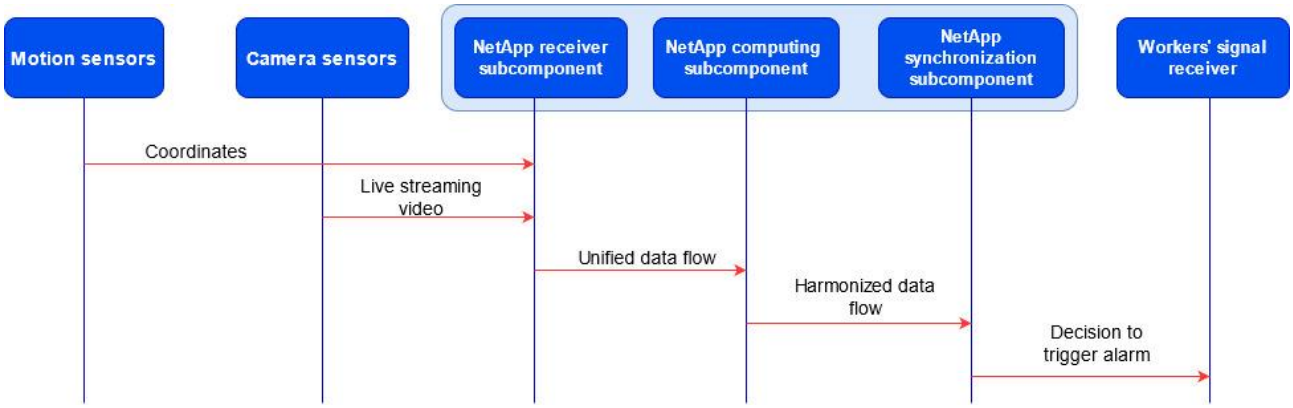

Figure 5-7 Flow of information to the NetApp for UC2

5.2.4 Data flows and management

It is expected for the NetApp to be functioning on a continuous mode, based on its monitoring nature and functionality. During its functional lifecycle, the NetApp is expected to collect input information at a specific and predefined rate. In this subsection, we will be discussing about the incoming data, their sources, and how they will be processed, managed, and secured through a normal operation of the NetApp itself.

Starting from the source of information, as previously stated, there are two main sources of incoming data, towards the NetApp, and one secondary. The two main sources namely are a) the Camera Unit (Jetson computing unit and the Camera sensor) and b) the Ultrawideband tags (the UWB anchor and the sensor tags). Both sources are expected to collect information about the environment (the camera unit) and the worker's movement (the UWB tags).

Each Camera unit consists of two components, the camera sensor, and the Jetson Unit. More specifically, the camera sensor is capturing images which are streamed straight to the Jetson Unit. In the Jetson, an image processing procedure occurs and detects when a subject (human, tool, etc.) is present in the scene. Once a present subject is observed, a bounding box enclosing the subject is calculated. Upon that event, the information regarding the bounding box is logged and transmitted towards the NetApp. Consequently, the NetApp will be receiving the relevant information about the coordination of the bounding box in the reference frame.

Table 5-2 UC2: Camera Unit source data

Data ID	Data Description	Data Type
messageID	A string value for the received message	String
cameraID	The ID of the camera unit	String
timestamp	The timestamp when the detection occurred	Timestamp
detectionID	The ID of the detection	String
z	A value for the z axis of the detection	Float
boundingBox	X,Y coordinates of the detected bounding box	Float

Moving to the UWB tags, each sensor tag will be worn to the wrist of each worker, and it is expected to transmit the exact location of the worker to its anchor. At this point we must clarify that each sensor tag is paired to its corresponding anchor. An anchor is the relevant H/W component which responsible to collect the transmitted data from the UWB sensor tag. Afterwards, the anchor transmits the data to the NetApp.

Table 5-3 UC2: UWB unit source data

Data ID	Data Description	Data Type
LEN	Length	Int
IMU	Inertial Measurement Unit	Not defined yet
DEVID	Device ID	String
TIMESTAMP	The timestamp of the measurement	Timestamp
SEQ	Sequence	Int
XACC	X-direction acceleration	Float
YACC	Y-direction acceleration	Float

Data ID	Data Description	Data Type
ZACC	Z-direction acceleration	Float
TEMP	Temperature	Float
HUMI	Humidity	Float

Lastly, as we mentioned above, there is one more source of information for the NetApp. This additional source is the delimited area coordinates that the safety administration is expected to provide for the NetApp. This additional input is expected to be delivered in the form of configuration. Meaning that for the NetApp to function as expected, the relevant delimited area has to be properly assigned.

Table 5-4 UC2: Safety Area source data

Data ID	Data Description	Data Type
AreaID	ID of safety area	Int
AreaName	Name of safety area	String
Coordinates	The coordinates of the safety area	JSON

Having presented all the needed information about the data sources, we can move on to the NetApp's data collection process. For each data source, three in total, the NetApp is expected to implement a separate component namely a) camera input component, b) UWB component, c) safety area component. For the main data sources, components a) and b), relevant REST APIs will be developed in order to consume the information provided from both ends. At this point, both sources are also expected to have the relevant REST endpoints for the NetApp to consume. As for the safety area, the NetApp will implement a parsing mechanism capable to read from an incoming file (.txt, .csv, etc.)

The processing of the incoming data is the step that follows the NetApp data collection process. The processing part will be divided into three separate stages namely, a) incoming data normalization, b) data fusion / synchronization, c) position evaluation / decision making. Starting with the first step, once data will flow towards the NetApp, a preprocessing component will be responsible to normalize the information based on rules which will be decided upon analysis of the data, Namely, we are expecting date format normalization, coordinates normalization and other metrics which will be provided by both streams of data. The second stage will be the synchronization component. In this component, the two data streams will be combined into one data stream based on rules and similar features. Finally, the decision-making component will be responsible to receive the synchronized stream of data alongside the safety area information from the configuration and manage to determine if there is a violation on site. Whether there is a violation or not, an alarm signal will be triggered to inform the administration and the workers about the issue.

Table 5-5 UC2: Preliminary NetApp KPI Analysis

Title	Description
Response Time (in milliseconds)	
From input to Sync	the time it takes for the data from the source to be available to the NetApp
From Sync to alarm	the time it takes for the NetApp to evaluate a measurement and trigger the alarm in case of a violation

Title	Description
NetApp performance (percentage)	
Results Accuracy	the accuracy of the results provided by the NetApp in case both source are available for measurements
Camera Accuracy	the accuracy of the results provided by the NetApp in case only camera source is available for measurements
UWB tags Accuracy	the accuracy of the results provided by the NetApp in case only tag source is available for measurements
False positive Rate	The rate of measurements which were false evaluated as area violations
Precision	True Positives / (True Positives + False Positives)
Component Availability (seconds)	
Frontend	the amount of time that the NetApp could tolerate in case of a Front End unavailability
Backend	he amount of time that the NetApp could tolerate in case of a Back End unavailability
Synchronization	the amount of time that the NetApp could tolerate in case of a Synchronisation component unavailability

Having in mind all the NetApp processing steps, it is important to mention that a separate component will be also implemented. This additional component will be responsible to evaluate the result information and calculate the predefined functional KPIs of the NetApp. The KPIs will also be displayed on a dashboard, for the administration to be able to evaluate and compare the benefits of the NetApp.

For better understanding, Figure 5-9 portrays the detailed data flow diagram portraying the NetApp data collection process, the data processing stages and the flow of the resulted information.

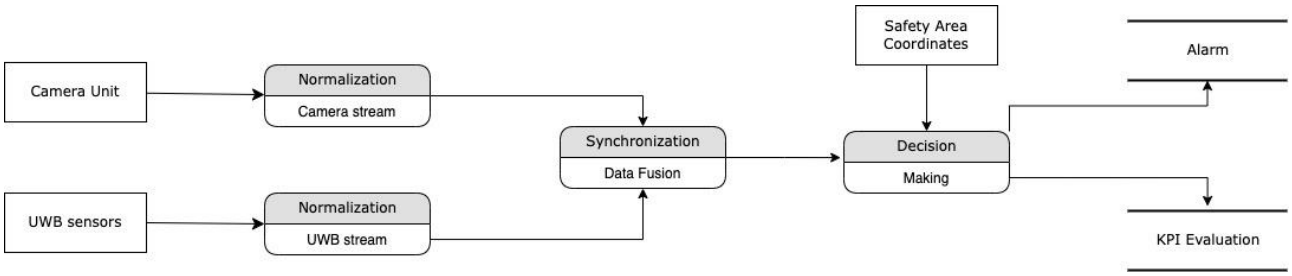

Figure 5-8 Data flow between NetApp's subcomponents

Moving on, below we will provide further insight on how the NetApp will be handling the collected and processed data in a secure manner. More specifically, during the data gathering, no personal information of the workers is collected. This conclusion is easily drawn from the fact that neither the camera unit delivers actual footage towards the NetApp, nor the sensor tags transmit any indicative personal information which could identify the worker. So, it is safe to assume that there is no specific reason by which we need to consider special constraints for the protection of personal information. Also, we have to keep in mind that the information from and to the NetApp will be transmitted within the reach of a private and secure 5G network deployed on a remote substation. As for the stored information, the NetApp is expected to keep records only from the safety area violations, such as date and time of the incident etc. Lastly, regarding

the KPI evaluation, even though each measurement/result (either violation or not) will be taken into consideration, only the actual KPI values will be stored for a specific amount of time. The incoming data streams will be discarded upon each measurement and result from the NetApp.

Future extensions of the system could provide external access to the results of the NetApp. As previously explained, each result of the NetApp will only indicate the time and space where the incident occurred without exposing any specific worker-related information. Hence, theoretically, an external service could consume the NetApp results (taking into consideration that the relevant endpoints will be developed) without knowing who the worker was or what lead to the incident.

5.3 NetApp UC3

The scope of this UC is the millisecond-level precise distributed generation monitoring, which addresses the domain of the distributed energy operation and maintenance with a specific focus on renewables. Specifically, in the context of this UC, the real-time monitoring of a wind farm is going to be performed by using the emerging capabilities of 5G telecommunication networks.

The high stochasticity of DER provokes significant problems in the operation of both transmission and distribution grids, where issues regarding voltage stability, congestion management, and frequency regulation are augmented. In addition, the steadily decreasing power system physical inertia (due to the reduction of synchronous generators), necessitates the operation of very fast frequency regulation services (such as the Fast Frequency Response service in Nordics with full activation time of 700 ms for 0.5 Hz deviation[37] and the dynamic containment in United Kingdom with full activation time of less than 1s[38]). The participation of DERs, such as battery storage assets, wind farms, IoT-enabled devices for demand response activation, etc., in those innovative services through electricity market frameworks, requires both orchestration (optimization of assets setpoint) and assets full activation in sub-second latency, in order to meet the strict temporal requirements for service provision. In addition, DER aggregators, and BRPs shall be able to balance their portfolio in hard-real time conditions, eliminating any imbalances introduced in the high-RES penetrated power system, and thus saving money from heavy balancing costs (avoidance of imbalance penalties). Therefore, the introduction of 5G can reduce significantly the time needed for both the monitoring and activation of signals to arrive from and to the field assets, while ensuring reliability and last mile connection in remote areas.

High-granularity precise monitoring of the real-time power production will offer the capability to wind farm owners to minimize their cost and, at the same time, being eligible for provision of ancillary and innovative flexibility services (voltage regulation, congestion management, etc.) through flexible plant management. In addition, this UC will demonstrate a working solution of a distributed RES generator/producer, which could be adopted and implemented on a bigger scale for other RES producers during the post project market exploitation stage. The strict requirements set by power system operators for the service provision by RES, render essential the utilization of high reliable and secure telecommunication connection between the physical asset (wind farm) and the dispatch centre of the operator. The wind farm is in South-eastern Bulgaria – Silven region. Since current 5G coverage does not reach the physical location of the wind farm, a real-time synchronized representation of the actual asset, i.e., wind farm, will be developed in Vivacom's (Bulgarian telecommunication Operator) 5G Lab.

In this UC, the specific location of the wind farm is South East Bulgaria – Sliven region. On September 21, 2020, VIVACOM announced the launch of its 5G network in all 27 district cities. This is the first stage of the introduction of the new technology which works simultaneously in the same frequency for both 4G and 5G – Dynamic Spectrum Sharing (DSS) in N3 (1800 MHz) frequency band. In 2021, VIVACOM have acquired N78 (3600 MHz) frequency resources and intensive rollout process was initiated in all settlements with population over 5000 inhabitants. 5G infrastructure rollout implies an intensive capital expenditure to introduce the technology. It is not financially viable to deploy in all geographic places at one time, e.g., in rural areas for residential, agricultural or industrial use. The issue is related to the need of many base stations all over the place to deliver consistent coverage. Since current 5G coverage does not reach the physical location of the wind farm, a real-time synchronized representation of the actual asset, i.e., wind farm, will be developed in the Vivacom's (Bulgarian telecommunication Operator) lab in Sofia, where 5G is already available for commercial use

5.3.1 Architecture

The UC3 NetApp consists of two components, namely the **predictive maintenance** and the **real-time energy production monitoring**. Each one of these components is implemented as a different VNF, which is interconnected and interacts with the inputs, and provides the necessary outputs to fulfil the functional requirements of this UC, as described in Figure 5-9.

The **predictive maintenance VNF** has two external CPs, one as an input to collect the data from the Raspberry Pi [115] supporting 5G connectivity, located at the Vivacom lab, and the other one as an output to provide the outcome of the internal processes to the wind farm owner.

The **real-time operation VNF** has two external CPs, one as an input to collect the data from the Raspberry Pi supporting 5G connectivity, located at the Vivacom lab, and one as an output to inform both the wind farm owner and operator about real-time production.

The two components have a management CP in order to grant access for configuration or debugging purposes.

The architecture for the NetApp is depicted in the following figure.

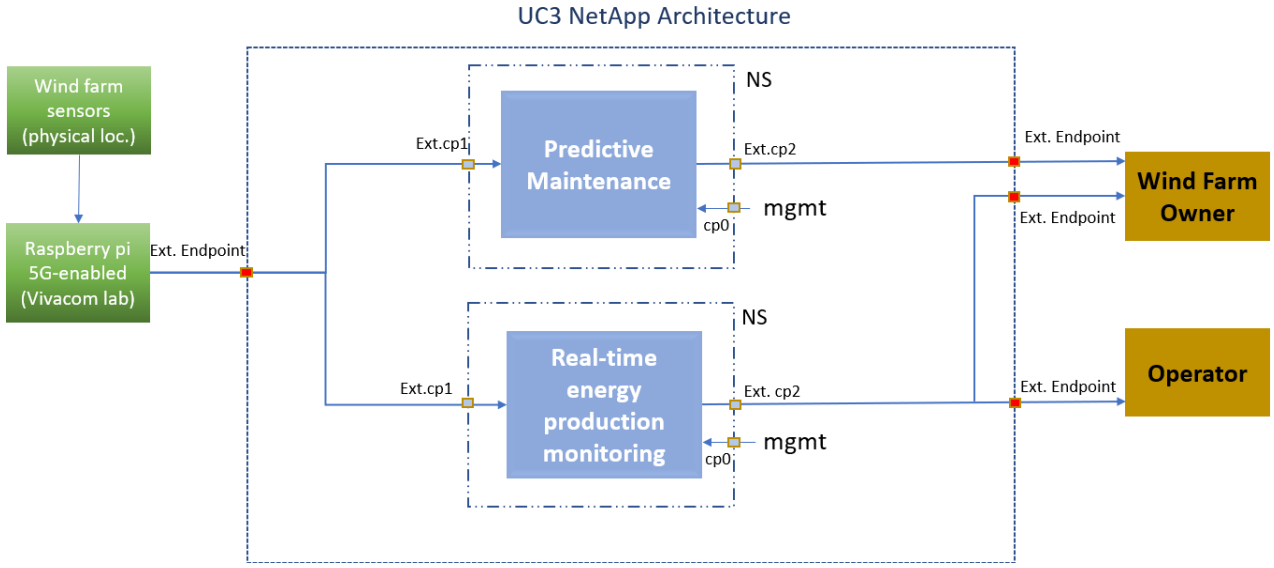

Figure 5-9 UC3 NetApp architecture

5.3.2 Software Components

The **predictive maintenance** component offers maintenance capabilities to the wind farm owner, leveraging the data measured from the sensors existing in the wind farm, which is then forwarded through Open Platform Communications (OPC) server to Vivacom's lab. The data generation process is repeated in a Raspberry Pi supporting 5G connectivity. OPC Unified Architecture (OPC UA), which is a machine-to-machine (M2M) communication protocol for industrial automation developed by the OPC Foundation, will be used as communication protocol in the context of this use case. Afterwards, this component collects the data, and makes them available for execution of an internal process to assess the wind farm operation to conclude whether any predictive maintenance action has to be taken. This internal assessment process and respective algorithms are to be developed in the post-project market implementation phase by an interested 3rd party provider (for example turbine maintenance service provider or OEM who has access to sufficient historical data to "train" the algorithms, Wind farm owner should receive the input from that component, increasing its capability to operate properly the asset. Regarding the wind farm performance monitoring, key performance parameters (such as turbine rotation and vibration) are collected from field sensors. Moreover, environmental parameters (such as wind speed, humidity, and ambient temperature), along with electrical parameters (such as power output, grid frequency, and voltage), are measured.

The **real-time energy production monitoring** provides real-time data monitoring of the wind farm production in a millisecond latency basis to the owner and the system operator. The data collection process follows similar approach as the previous described component.

5.3.3 Scenario description

The measurements from the wind farm sensors are sent through the OPC server to the Raspberry pi 5G-enabled, located at VIVACOM's lab. The NetApp is hosted in a cloud server and performs the functionalities described above. Some demonstration scenarios regarding the vertical service provided by the UC3 NetApp are:

- There is no abnormality detection in the wind farm operation, thus no alerts are sent to the wind farm operator.
- There is an identification of potential operation failure in the wind farm in the near future, and predictive maintenance information is sent to the wind farm owner.
- There is an availability issue of the wind farm in real-time (stop operating), and information is sent to both system operator and wind farm owner.
- Real-time production does not introduce any burden to the power system operator, thus no alerts are sent to the wind farm operator nor to the power system operator.
- Real-time production of the wind farm provokes system stability issues, and thus the system operator shall curtail the operation of wind farm.

More information regarding the scenario's description has been given in D2.1 of Smart5Grid and especially in section 3.4. A brief information flow diagram is provided below.

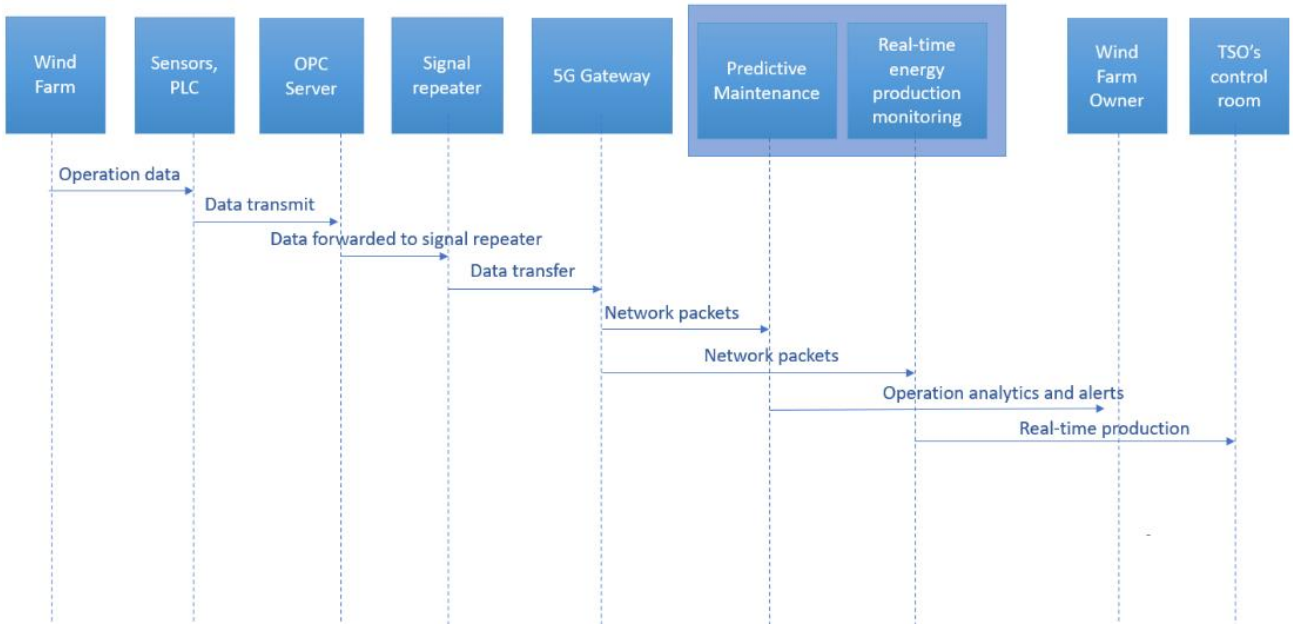

Figure 5-10 Flow information diagram for UC3

5.3.4 Data flows and management

In this subsection, we will be discussing about the incoming data, their sources (SCADA and third-party sensors), data flow and how they will be processed, managed, and secured through a normal operation of the NetApp itself.

There are two sources of incoming data towards the NetApp namely a) the SCADA (Supervisory Control and Data Acquisition) system and b) third-party sensors (vibro-sensor). The first source (SCADA) provides information about different parameters of wind farm's operations – technical, electrical, environmental and the vibro-sensor will send in high frequency additional technical data about the asset performance. Apart from it being the first solution of this type (IoT in 5G), the innovation here is also incorporating different sources of information into a single NetApp.

The real-time measurements stemming from the wind farm are included in the following signal list. This extensive list might slightly change in the course of the NetApp development.

Table 5-6 UC3: Measurement data

Data ID	Description	Data Type
AlmActSt	Alarm status (0 = no alarm, >0 = Alarm number)	Long Integer
GriA1	Grid side phase 1 current	Single Float
GriA2	Grid side phase 2 current	Single Float
GriA3	Grid side phase 3 current	Single Float
GriHz	Frequency	Single Float
GriPF	Grid side 3 phase power factor	Single Float
BrgTmp1	Generator Bearing Drive End temperature	Long Integer
BrgTmp2	Actual bearing Non Drive End temperature	Long Integer
ClWtrPmpPres	Generator cooling water pump pressure	Single Float

Data ID	Description	Data Type
ClWtrTmp	Generator cooling water temperature	Long Integer
ClWtrTnkPres	Generator cooling water tank pressure	Single Float
RotPNV1	Generator rotor phase1-to-neutral voltage	Single Float
RotPNV2	Generator rotor phase2-to-neutral voltage	Single Float
RotPNV3	Generator rotor phase3-to-neutral voltage	Single Float
RotSpd	Rotational speed	Single Float
RotTmp1	Temperature measurements for generator rotor, phase 1	Long Integer
RotTmp2	Temperature measurements for generator rotor, phase 2	Long Integer
RotTmp3	Temperature measurements for generator rotor, phase 3	Long Integer
Var	Generator reactive power	Single Float
W	Generator active power	Single Float
EnvTmp	Temperature of environment	Long Integer
HorWdSpd	Horizontal wind speed	Single Float
HorWdSpdEst	Horizontal wind speed estimated	Single Float
AcuAlmSt	Nacelle Acoustic alarm status (1 = Started)	Boolean
IntnTmp	Temperature inside nacelle	Long Integer
CoreTmp1	Temperature core, phase 1	Long Integer
CoreTmp2	Temperature core, phase 2	Long Integer
CoreTmp3	Temperature core, phase 3	Long Integer
TurTmp1	Temperature on turbine side, phase 1	Long Integer
TurTmp2	Temperature on turbine side, phase 2	Long Integer
TurTmp3	Temperature on turbine side, phase 3	Long Integer
ClWtrLev	Gear cooling water level	Single Float
ClWtrPmpPres	Gear cooling water pump pressure	Single Float
ClWtrTmp	Gear cooling water temperature	Long Integer
ClWtrTnkPres	Gear cooling water tank pressure	Single Float
GbxBrgTmp1	Actual gear bearings temperature A (Rotor end)	Long Integer
GbxBrgTmp2	Actual gear bearings temperature B (Generator End 1)	Long Integer
GbxBrgTmp3	Actual gear bearings temperature C (Generator End 2)	Long Integer
GbxOilTmp	Measured temperature of gearbox oil	Long Integer
DateTm	Actual date/time	Date
TotVArh	Total (net) reactive energy production	Long Integer
TotWh	Total (net) active energy production	Long Integer
Vibrosensor	Vibrosensor on gear box or/and generator	tbd (depending on sensor's the supplier - recruitment in process)

The incoming data will be processed online in five stages namely:

a) data validation – checking source, time stamp, availability of data, etc.

b) data parsing and categorization – every signal will be categorized in three types of data (technical, environmental, electrical) with the aim of better further visualization.
c) data analysis and visualization – based on the data category and the user's role, the data will be visualized in a manner to provide the best usability and value.
d) data exceptions analysis and notifications – the received and visualized data will be analyzed in terms of predefined rules and values thresholds and alarm signals will be triggered to inform the respective users in case the real data outreaches the predefined limits.
e) data storage - the data will be stored for the purposes of further analysis especially as a mean for enabling future development of predictive maintenance algorithms or other statistical/analytical functionalities.

Figure 5-10 describes the exact flow of data within the NetApp, which described in more details is the following:

1) The measurements from the wind farm sensors and SCADA system are sent through OPC server over VPN to a 5G-enabled Raspberry Pi located at the VIVACOM's lab. Thus, a digital replication on the wind farm (signal list) is created in an area with 5G coverage in a secure manner.
2) A 5G connected IoT device (Raspberry Pi with 5G HAT) sends from the digital replica of the Wind farm signals to the UC3 NetAapp through Vivacom's public 5G network.
3) The UC3 NetAapp reads signals from IoT device using MQTT protocol. The advantages of MQTT are:
   a) Lightweight and Efficient: MQTT clients are very small, require minimal resources so can be used on small microcontrollers.
   b) Bi-directional Communications: MQTT allows for messaging between device to cloud and cloud to device.
   c) Scale to Millions of Things: MQTT can scale to connect with too many IoT devices.
   d) Reliable Message Delivery: Reliability of message delivery is important for many IoT use cases.
   e) Support for Unreliable Networks: Many IoT devices connect over unreliable cellular networks. MQTT's support for persistent sessions reduces the time to reconnect the client with the broker.
   f) Security Enabled: MQTT makes it easy to encrypt messages using TLS and authenticate clients using modern authentication protocols.
4) The data is displayed with ASP.NET Web P-Pages (Razor) and JavaScript
5) The data is made accessible to the UC3 NetApp users based on the authorization rules related to their user roles:
   a) Asset Owner
   b) TSO
   c) Administrator
   d) Viewer (partners involved in the demo activities

5.4 NetApp UC4

The scope of this UC4 is the real-time monitoring of a geographical wide area where cross-border power exchanges take place. The UC4 addresses the energy reliability and security domain of the broad energy vertical. Specifically, in the context of this UC, the interconnection flow between Greece and Bulgaria is monitored, leveraging the advantages that 5G telecommunication infrastructure provides. This function can be executed from the newly established RSC in Thessaloniki, Greece. The role of the RSC is to promote regional cooperation and to support the strengthening of the neighbouring power systems and market operations in the region. To achieve the enhancement of the interconnected power system operation, live

monitoring of the power flows between the countries under its area of interest is of vital importance. Hence, this UC can be considered as the development of an additional element that increases the live monitoring capability of the RSC. PMUs located at the High Voltage network of the Northern Greece and Bulgaria, monitoring the interconnection between the two areas, can be used as an input in the monitoring process of the RSC. Those advanced metering devices offer time-stamped measurements of phasors of voltage and current with high data granularity (50 to 60 times per second) enabling the in-depth analysis of the positive, negative and zero sequence phasors. These measurements are then collected from the aforementioned PMUs, aligned, and stored by a PDC. In the context of this UC, a vPDC will be developed for this data gathering process and incorporated as the pivotal part of a NetApp that leverages the 5G technological advancements. The utilization of 5G, enables the virtualization of grid components such as the PDC, providing the connectivity between a vPDC and the PMUs, and offering the low latency and high reliability needed, due to the criticality of the UC. The latency´s constraint is not crucial for the monitoring application that is implemented in the project's scope. However, it is taken into consideration as it will facilitate demanding applications, such as state estimation, oscillation detection and control, voltage stability control, load modelling validation, and system restoration and event analysis [116]. Hence, the NetApp envisioned to be developed in the context of this UC, in order to fulfil the above-mentioned objectives, will cover three types of services: vPDC Service, Monitoring Service (WAM) and Advisory Service to the involved TSOs.

5.4.1 Architecture

As mentioned above, the NetApp consists of three components: the vPDC, the Monitoring Service, and the Advisory Provisioning Service. Each one of these components is implemented as a different VNF, which is interconnected and interacts with the rest of them.

The vPDC VNF has an external CP, the input from the PMU. Then, after the processing of the data described in section 5.4.2, the output will be made available to the other blocks via the internal CPs.

The Monitoring VNF has an internal CP, the input from the vPDC, as well as one CP to communicate with the Advisory VNF.

The Advisory VNF has two internal CPs, the inputs given from the other two VNFs, and an external one to provide the advice messages to the TSOs.

All three components have a management CP in order to grant access for configuration or debugging purposes. For the Monitoring VNF, the management CP will also be used for the RSC (owner and administrator of the NetApp) to have access to the visual representations that will be explained in the section below.

The architecture for the NetApp is the one proposed in the following figure.

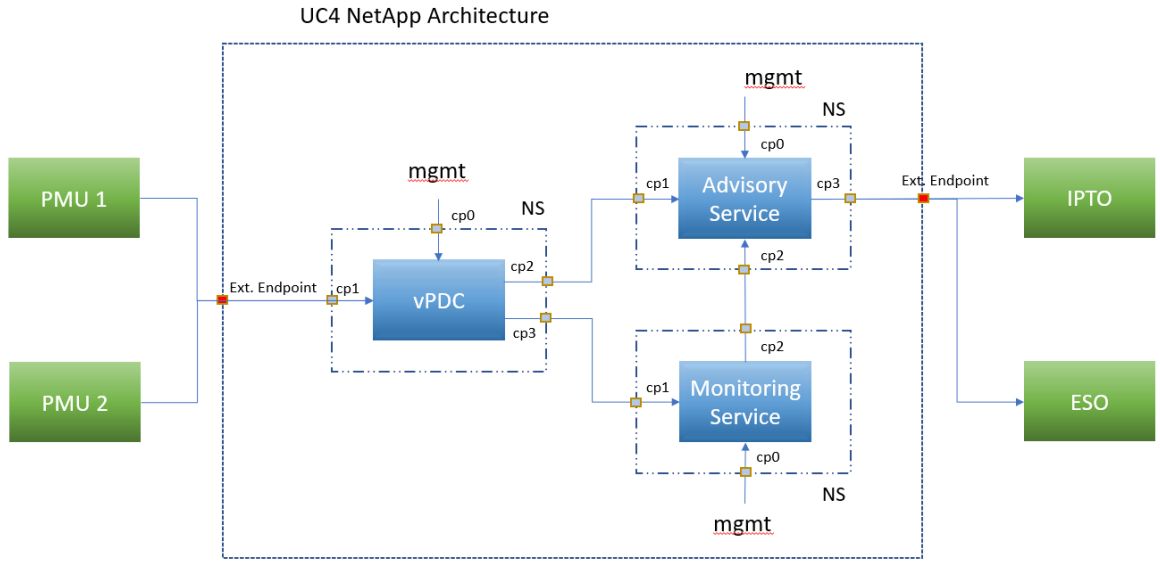

Figure 5-11 UC4 NetApp architecture

5.4.2 Software components

The **vPDC service** will include several functional requirements to preserve the standards and the constrains implied by the application of WAM, as dictated by the IEEE C37.244 standard [117]. Those could be summarized as follows:

1. **Data aggregation with time alignment to relative time:** The PDC aligns data received from PMUs or lower level PDCs, creates new packets with the measurements with the same timestamp and transmits the combined data in one or more output data streams to other PDCs or applications such as archiving, visualization, or control. The PDC latency starts when the first measurement from one of the PMUs with a given timestamp arrives at the PDC. Then the PDC waits for the rest of the measurements with the same timestamp to arrive, until the waiting time expires.). Any data that arrives later than the end of the relative wait time is lost. A more detailed description of the PDC waiting time can be found in D2.1 and IEEE C37.244 standard. The E2E PDC latency can be thought of as the difference between the time of egress of the output data, minus the time of the first data arrival at the PDC. This latency will be approximately the relative wait time, plus the PDC processing time (alignment and aggregation). Hence, the balance between the data lost and the waiting time for all the measurements to arrive is crucial to be inspected. The low latency provided by the 5G network decreases the time for the data to arrive from the PMUs, and thus decreasing the waiting time of the vPDC and the overall processing time.
2. **Data validation:** A PDC may perform basic data validation and checking of the data arriving at the PDC. This includes checking the data status flags and time quality of all PMUs and performing data integrity checks on all received data.
3. **Data transfer protocol support:** PMU data may be available in different synchrophasor data transfer and communication protocols such as IEEE Std C37.118.2-2011, IEEE Std C37.118-2005, IEEE Std 1344-1995, IEC 61850-90-5, and new profiles as they become defined. This requirement will be valid in case that more than one data transfer protocol, i.e., incompatible PMUs from different

vendors, is used in the demonstrators. In the specific UC the newest version of C37.118 protocol at the time of development will be used.

4. Output data buffering: A PDC may buffer output data to reduce data losses in case communication to other PDCs or applications is interrupted. This function affects PDC memory requirements.

- Configuration: Configuration management is designed to assure availability of appropriate data for the local functions of the PDC as well as other applications that receive data from the PDC. Configuration information is sent by the data source to the data destination ahead of the actual data to permit the data destination to interpret the data as soon as it arrives. The configuration information may be sent unsolicited, or on explicit requests.

5. Performance monitoring: A PDC may have performance monitoring functions to monitor quality of data and communication with other PMUs and PDCs. Performance monitoring includes errors, events, and overall system operation

   Performance monitoring may include logging of:

   a. Total number of measurements not received but expected.
   b. Measurements received with values out of range, per absolute range checks or model-based data validation.
   c. The quality of received synchro phasor data.
   d. Measurements received but corrupted.
   e. Good data received, but with a bad timestamp so it cannot be integrated as expected
   f. Good data.

6. Cyber security: Cyber security will be evaluated by all PDC interfaces, while maintaining the reliability of the service. PDC cyber security likely goes beyond simply securing synchrophasor communications, but any communications and access to the PDC. Security practices that are poorly applied to PDCs may degrade PDC performance and/or functionality.

The Monitoring Service (WAM) will demonstrate several status indicators and visualization features of the PMUs. Those features are:

- A map indicating device's location in the power system.
- The device's name, address, model, serial number, and firmware version.
- The nominal grid frequency [Hz] and the current reporting speed [fps].
- Real-time phase diagram with voltage and current vectors.
- Voltage magnitude and angle difference monitoring, deriving from historical data of both sites.

Finally, the Advisory Service will implement an algorithm and, according to its results, it will inform the two operators that corrective moves need to be done in case of an abnormality in the grid. This fault detection algorithm could come from the Signal Processing field or from the Artificial Intelligence field.

As for the constrains that the three components introduce in the system, the vPDC needs the data from the PMUs to arrive as fast as possible (low latency) and without many packet losses. This will increase the observability of real time interconnected power system. The data aggregation that it will implement is not a heavy computational process, as it only compares the timestamps of the incoming data and matches them with the identical ones. The WAM service will need more computational power to construct the diagrams in comparison with vPDC, but, since the time constrains change to s from ms, the networking needs get relaxed. Finally, the Advisory Service will need both computational and networking power, as it is going to provide the results and deliver them to the TSOs in hard real time.

5.4.3 Scenario description

The PMU devices, mounted on the two sides of the interconnection line between Greece and Bulgaria, get the measurements and forward them to the edge-cloud server, hosting the NetApp. Inside the server, the vPDC will synchronise the measurements and pass them to the Monitoring and the Advisory Services. The scenarios to be detected and get examined in the UC's NetApp are the following:

- No abnormality detected in the grid operation (normal operation), so no suggestion provision occurs.
- Detection of Rate of Change of Frequency (RoCoF) abnormality, suggestion to both TSOs provisioned.
- Detection of abnormalities in voltage and current phasors, suggestion to the related TSO is provisioned.

The procedure of instantiation of the NetApps, as well as their normal operation as network services can be found in Smart5Grid deliverable D2.1.

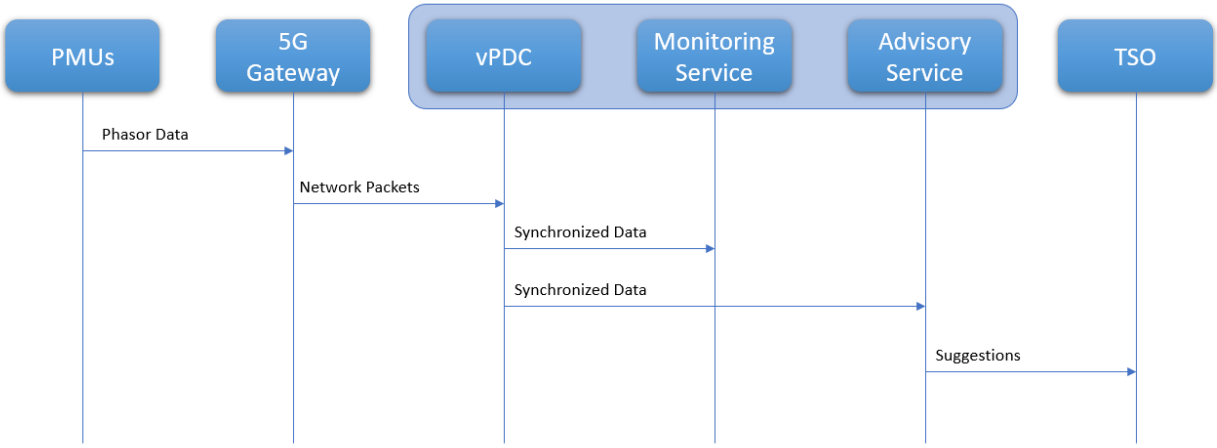

Figure 5-12 Flow of information to the NetApp for UC4

5.4.4 Data flows and management

The Data Flow of the UC begins with the PMUs collecting measurements of voltage and current of all three phases of the system and the frequency of the grid. Those measurements get timestamped and then they are transmitted to the edge/cloud server and specifically to the vPDC Service. Table 5-7 shows each of the items of data that will be collected from each PMU at every slot of time.

Data ID	Data Description	Data Type
PhasorDate	Date	Date time
PhasorTime	Time	Hour Time
PhasorMs	Time in ms resolution	Integer
PMU#GpsReliable	GPS Reliability	Integer
PMU# UPhase1abs	Absolute Amplitude of Voltage in Phase 1	Floating
PMU#UPhase1phase	Phasor of Voltage in Phase 1	Floating
PMU#UPhase2abs	Absolute Amplitude of Voltage in Phase 2	Floating
PMU#UPhase2phase	Phasor of Voltage in Phase 2	Floating
PMU#UPhase3abs	Absolute Amplitude of Voltage in Phase 3	Floating

Data ID	Data Description	Data Type
PMU#UPhase3phase	Phasor of Voltage in Phase 3	Floating
PMU#IPhase1abs	Absolute Amplitude of Current in Phase 1	Floating
PMU#IPhase1phase	Phasor of Current in Phase 1	Floating
PMU#IPhase2abs	Absolute Amplitude of Current in Phase 2	Floating
PMU#IPhase2phase	Phasor of Current in Phase 2	Floating
PMU#IPhase3abs	Absolute Amplitude of Current in Phase 3	Floating
PMU#IPhase3phase	Phasor of Current in Phase 3	Floating
PMU#Freq	Frequency value	Floating

Table 5-7. UC4 - Data collected from PMUs, processed and stored at the vPDC

The vPDC processes all the measurements arriving within the accepted time windows (waiting time) from the multiple PMUs and then formats the new packets with the measurements of same timestamp. The resulting packets are then forwarded to the Monitoring and the Advisory Service. There the visualization takes place, and if needed, the Advisory Service provides alerts to the two TSOs. Figure 5-12 describes the exact flow of data within the NetApp and the process details by each component have been described in Section 5.4.2

The information received by the vPDC, apart from being online processed, it is also stored in a database (inside the vPDC Service) for historical data to be available for e.g., post analysis of abnormal events or creation of digital twin of the energy grid.

In context of security of the data managed by the Netapp, each system operator, namely IPTO and ESO, will only be able to access the data from its own PMU devices. The entity that has access to the PMU data stemming from the transmission systems of both Operators is the RSC, which is owner of the NetApps. For the purposes of the Smart5Grid project, the role of RSC is impersonated by both of the engaged in the UC#4 Operators.

Furthermore, the data transmission from the PMU devices to the NetApp is protected by the 5G network. The 5G solution to be exploited by the demo trials shall be aligned with the wider scope of the 5G Security requirements described in 3GPP Release 16 ([119], [120]) and in 3G PPP Release 17 [121], the following security domains are synoptically described :

1 Network access security domain, which is the set of security features that enable a UE (in UC4 Greek demo it will be a Zyxel Gateway Router) to authenticate and access services via the network securely and to protect against attacks on the radio interfaces
2 Network Domain Security, which is the set of security features that enable network nodes to securely exchange signalling and user plane data.
3 User Domain Security, which is the set of security features that secure the user access to the mobile stations and to the mobile equipement in particular.
4 Application domain security ,which is the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.
5 SBA (Service Based Architecture) domain security, which is the set of security features that enables network functions of the SBA architecture to communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces.

6 **Visibility and configurability of security,** which is the set of features that enable a user to be informed whether a security feature is in operation or not, and whether the use and provision of services should depend on the security feature.

6 Conclusions and next steps

The main outcome of this document has been to define the Smart5Grid NetApp concept and the platform architecture, its components, and the interactions between them. As in any modern software projects, requirements and definitions will be continuously reviewed on the subsequent tasks to refine the results; updates/changes will be highlighted in upcoming deliverables if necessary.

To achieve this goal, first, we reviewed the state of the art and other initiatives relevant to the project, so as to set a strong foundation for the design and specification work undergone. Smart5Grid will support most of smart grid´s functionalities by enabling an environment in which cloud-native NetApps can realize the integration between the energy vertical and 5G networks, with a special focus on deployments that leverage edge infrastructure. As we have reviewed in depth, many 5G PPP projects from previous phases have published outcomes that serve as a starting point for Smart5Grid and, furthermore, the outcomes of more recent projects will be closely monitored to guarantee a strong alignment with them.

Furthermore, this document presented the new concept of NetApp as envisioned by Smar5Grid. This is, as we have learnt, being addressed on several projects with multiple approaches. The common point between them is highlighted as the need to ease the barriers for vertical application developers when working with 5G networks, abstracting them from the complexities of latest generation telecommunications networks. The Smart5Grid NetApp is defined conceptually as a chain of cloud-native VNFs that are chained together into services, and defined in a NetApp descriptor that specifies both network and service specific requirements, thus abstracting the developer from the implementation of said requirements.

This NetApp concept served as the basis for the Smart5Grid architecture design also presented in this deliverable3.2. The designed Smart5Grid Experimental 5G platform enables 3rd party developers to implement, verify and validate NetApps, before making them available to other users of the platform. To enhance this main functionality, the designed V&V platform and OSR, adopt the DevOps cycle paradigm, which expedites software delivery and reduce time-to-market for robust and fully tested applications.

4A deep dive into each of the three layers that compose the architecture (i.e., Platform, NFV/Telco, and Energy) was also provided, describing its components, their functionality, and the interactions among them. Together with the specification of these components, we presented the first version of the formal specification of Smart5Grid NetApps in a descriptor that offers the flexibility required to fulfil the requirements outlined by the UCs in previous deliverable D2.1.

And finally, an updated description of each UC in the project was presented, with special focus on the NetApp that will be developed within it according to the presented NetApp specification.

The work presented in this deliverable provided the necessary input for the upcoming tasks and enables the project to take its next steps. Within WP2, T2.4 will focus the attention on the alignment of Smart5Grid with previous 5G-PPP phases and establish a roadmap for 3rd party experimentation. The ongoing WP3 and WP4 will take this input in order to develop a fully integrated network facility and repository, and boost the technology evolution required for NetApp development respectively. Finally, WP5 and WP6 will focus on the integration of the developed NetApps with the platform and the actual pilots on the field.

7 References

[1] Smart5Grid Project (2021). Smart5Grid deliverable D2.1 "Elaboration of Use Cases and System Requirements". Available at: https://smart5grid.eu/wp-content/uploads/2021/07/Smart5Grid_D2.1_Elaboration-of-UCs-and-System-Requirements-Analysis_V1.0.pdf

[2] Smart grid definition: https://en.wikipedia.org/wiki/Smart_grid

[3] Zahariadis, T., Trakadas, P., Skias, D., Leligou, H. C., Gikaki, A., Voliotis, S., Spada, M. R., Gonos, A, & Kanakis, E (2018). Smart Energy as a Service Network Architecture. In Proceedings of EuCNC-2018, pp.109-113, IEEE. Available at: http://www.nrg5.eu/wp-content/uploads/2018/07/EuCNC-NRG5_Zahariadis_1.pdf

[4] International Telecommunication Union – Radiocommunications Sector (ITU-R) (2015). Recommendation ITU-R M.2083-0 (09-2015): "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond". Available at: https://www.itu.int/rec/R-REC-M.2083

[5] Kepler/Cannon (2020). The Cloud-Native Paradigm. Evolving enterprises and the new business-IT convergence. Available at: https://www.keplercannon.com/cloud-native-paradigm/

[6] Gannon, D., Barga, R., & Sundaresan, N. (2017). Cloud-native applications. IEEE Cloud Computing, 4(5), 16-21.

[7] Hustad, E., & Olsen, D. H. (2021). Creating a sustainable digital infrastructure: the role of service-oriented architecture. Procedia Computer Science, 181, 597-604.

[8] VNF Forwarding Graph definition. Available at: https://docs.openstack.org/tacker/ocata/devref/vnffg_usage_guide.html

[9] ETSI (2018). ETSI GR NFV-IFA 028 V3.1.1 (2018-01): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains". Available at: https://www.etsi.org/deliver/etsi_gr/NFV-IFA/001_099/028/03.01.01_60/gr_NFV-IFA028v030101p.pdf

[10] J. Carapinha, J., Di Girolamo, M., Monteleone, G., Ramos, A., and Xilouris, G. (2016). VNFaaS with End-to-End Full Service Orchestration. In Proceedings of the 2016 Fifth European Workshop on Software-Defined Networks (EWSDN), pp. 57-58, IEEE. DOI: 10.1109/EWSDN.2016.19

[11] Zhou, X., Li, R., and Chen, T. (2016). Network Slicing as a Service: Enabling Enterprises' Own Software-Defined Cellular Networks. IEEE Communications Magazine 54(7), 146-153. DOI: 10.1109/MCOM.2016.7509393

[12] Duan, Q. (2021). Intelligent and Autonomous Management in Cloud-Native Future Networks—A Survey on Related Standards from an Architectural Perspective. Future Internet, 13(2), 42.

[13] Cloud Service Models: https://www.javatpoint.com/cloud-service-models

[14] 5G PPP (2020). 5G PPP Software Network WG Paper, "Cloud-Native and 5G Verticals' services". Available at: https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-SN-WG-5G-and-Cloud-Native.pdf

[15] VMware website: https://www.vmware.com/

[16] Virtualbox website: https://www.virtualbox.org/

[17] OpenStack website: https://www.openstack.org/

[18] ETSI (2014). ETSI GS NFV MAN V1.1.1 (2014-12): "Network Functions Virtualisation (NFV); Management and Orchestration". Available at: https://www.etsi.org/deliver/etsi_gs/nfv-man/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf

[19] ETSI "NFV Release 4 Definition". Available at: https://docbox.etsi.org/ISG/NFV/Open/Other/ReleaseDocumentation/NFV(21)000025_NFV_Release_4_Definition_v0_3_0.pdf

[20] CNCF Website: https://www.cncf.io/

[21] ETSI (2019) ETSI GR NFV-IFA 029 V3.3.1 (2019-11) "Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"". Available at: https://www.etsi.org/deliver/etsi_gr/NFV-IFA/001_099/029/03.03.01_60/gr_NFV-IFA029v030301p.pdf

[22] 5G PPP (2015)5G Vision, The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services". Available at: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

[23] ETSI (2015). ETSI White Paper No.11: "Mobile Edge Computing: A key technology towards 5G", September 2015. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

[24] ITU-R (2015). ITU-R Recommendation M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond", September 2015. Available at: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

[25] ETSI (2017). ETSI GS MEC 010-1 V1.1.1, "Mobile Edge Computing (MEC); Mobile Edge Management; Part 1: System host and platform management", October 2017. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/01001/01.01.01_60/gs_MEC01001v010101p.pdf

[26] ETSI (2019). ETSI GS MEC 010-2 V2.1.1, "Mobile Edge Computing (MEC); Mobile Edge Management; Part 2: Application lifecycle, rules and requirements management", November 2019. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/01002/01.01.01_60/gs_MEC01002v010101p.pdf

[27] ETSI (2017). ETSI GS MEC 011 V1.1.1, "Mobile Edge Computing (MEC); Mobile Edge Platform Application Enablement", July 2017, ETSI GS MEC 011. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/01.01.01_60/gs_mec011v010101p.pdf

[28] ETSI (2017). ETSI GS MEC 012 V1.1.1, Mobile Edge Computing (MEC); Radio Network Information", July 2017. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/012/01.01.01_60/gs_MEC012v010101p.pdf

[29] ETSI (2017). ETSI GS MEC 013 V1.1.1, "Mobile Edge Computing (MEC); Location API", July 2017. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/013/01.01.01_60/gs_MEC013v010101p.pdf

[30] ETSI (2018). ETSI GS MEC 014 V1.1.1, "Mobile Edge Computing (MEC); UE Identity API", February 2018. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/014/01.01.01_60/gs_mec014v010101p.pdf

[31] ETSI (2017). ETSI GS MEC 015 V1.1.1, "Mobile Edge Computing (MEC); Bandwidth Management API", October 2017. Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/015/01.01.01_60/gs_MEC015v010101p.pdf

[32] ETSI (2017). ETSI GS MEC 016 V1.1.1, "Mobile Edge Computing (MEC); UE Application Interface", September 2017. Available at: https://www.etsi.org/deliver/etsi_gs/mec/001_099/016/01.01.01_60/gs_mec016v010101p.pdf

[33] 3GPP (2018). 3GPP TS 23.501 V15.1.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15)"; March 2018. Available at: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/

[34] ETSI (2016). ETSI GS MEC 003 V1.1.1, "Mobile Edge Computing (MEC); Framework and Reference Architecture", March 2016.Available at: http://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_mec003v010101p.pdf
[35] 5G-PPP Website: https://5g-ppp.eu/
[36] 5G PPP - ICT-41-2020 - 5G innovations for verticals with third party services (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/ict-41-2020
[37] 5G-Transformer ("5G Mobile Transport Platform for Verticals") Project (Grant Agreement No.761536) website: http://5g-transformer.eu/
[38] MATILDA ("A Holistic Innovative Framework for the Design, Development and Orchestration of 5G-Ready Applications and Network Services over Sliced programmable Infrastructure") Project (Grant Agreement No.761898) website: https://www.matilda-5g.eu
[39] 5GASP ("5G Applications & Services experimentation and certification Platform") Project (Grant Agreement no.1010116448) website: http://5gasp.eu/
[40] 3GPP (2021). 3GPP, TS 23.222 V17.5.0 (2021-06), "Common API Framework for 3GPP Northbound APIs"; Stage 2 (Release 17)". Available at: https://www.3gpp.org/ftp/Specs/archive/23_series/23.222/
[41] 3GPP (2021). 3GPP, TS 23.434 V17.2.0 (2021-06), "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows"; (Release 17)". Available at: https://www.3gpp.org/ftp/Specs/archive/23_series/23.434/
[42] 5G-EPICENTRE ("5G ExPerimentation Infrastructure hosting Cloud-nativE Netapps for public protection and disaster Relief") Project (Grant Agreement No.101016521) website: http://5gepicentre.eu/
[43] 5G-EPICENTRE Project (2021). 5G-EPICENTRE deliverable D1.3: Experimentation requirements and architecture preliminary version. Available at: https://www.5gepicentre.eu/wp-content/uploads/2021/08/5G-EPICENTRE_D1.3_Experimentation-requirements-and-architecture-specification-preliminary-vesrion_v2.0_20210630_FORTH.pdf
[44] 5G-ERA (5G Enhanced Robot Autonomy") Project (Grant Agreement No.101016681) website: http://5g-era.eu/
[45] 5G-IANA ("5G Intelligent Automotive Network Applications") Project (Grant Agreement No.101016427) website: http://5g-iana.eu/
[46] 5G-INDUCE ("An open cooperative 5G experimentation platform for the industrial sector NetApps") Project (Grant Agreement No.101016941) website: https://www.5g-induce.eu/
[47] 5GMediaHUB ("5G Experimentation Environment for 3rd Party Media Services") Project (Grant Agreement No.101016714) website: https://www.5gmediahub.eu/
[48] 3GPP (2018). 3GPP, TR 28.801 V15.1.0. (2018-01): "Technical Specification Group Services and System Aspects; Telecommunication management; Study on management and orchestration of network slicing for next generation network (Release 15)," Available at: https://www.3gpp.org/ftp/Specs/archive/28_series/28.801/
[49] EVOLVED-5G ("Experimentation and Validation Openness for Long-term evolution of Vertical inDustries in 5G era and beyond") Project (Grant Agreement No.101016608) website: https://evolved-5g.eu
[50] VITAL-5G ("Vertical Innovations in Transport and Logistics over 5G experimentation facilities") Project (Grant Agreement No.101016567) website: https://www.vital5g.eu
[51] NRG-5 ("NRG-5 Enabling Smart Energy as a Service via 5G Mobile Network advances") Project (Grant Agreement No.762013) website: https://www.nrg5.eu
[52] 5G-VICTORI ('VertIcal demos over Common large scale field Trials fOr Rail, energy and media Industries") Project (Grant Agreement No.857201) website: https://www.5g-victori-project.eu

[53] 5GZORRO ("Zero-tOuch secuRity and tRust for ubiquitous cOmputing and connectivity in 5G networks") Project (Grant Agreement No.871533) website: https://www.5gzorro.eu/
[54] CARAMEL (Artificial Intelligence based cybersecurity for connected and automated vehicles") Project (Grant Agreement No.833611) website: https://www.h2020caramel.eu/
[55] 5GCity ("A Distributed Cloud and Radio Platform for 5G Neutral Hosts") Project (Grant Agreement No.761508) website: https://www.5gcity.eu/
[56] SHIELD () Project Grant Agreement No.) website: https://www.shield-h2020.eu/
[57] SELFNET ("A Framework for Self-Organised Network Management in Virtualized and Software-defined Networks") Project (Grant Agreement No.671672) website: https://selfnet-5g.eu/
[58] SONATA ("Service Programming and Orchestration for Virtualized Software Networks") Project (Grant Agreement No.761493) website: https://sonata-nfv.eu/
[59] OSM Website: https://osm.etsi.org/
[60] ONAP Website: https://www.onap.org/
[61] ETSI (2014). ETSI GS NFV-MAN 001, "Network Function Virtualisation (NFV); Management and Orchestration,"V1.1.1, December. 2014. Available at: https://www.etsi.org/deliver/etsi_gs/nfvman/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf
[62] Kubernetes website: https://kubernetes.io/
[63] Keystone, the Open Stack Identity Service website: https://docs.openstack.org/keystone/latest/
[64] Centos OS website: https://www.centos.org/download/
[65] Kubernetes Cluster on CentOS 7 with kubeadm Website: https://computingforgeeks.com/install-kubernetes-cluster-on-centos-with-kubeadm/
[66] Collectd website: https://collectd.org/
[67] Iperf website: https://iperf.fr/
[68] Cloudprober website: https://cloudprober.org/
[69] Kubernetes Node Feature Discovery website: https://github.com/kubernetes-sigs/node-feature-discovery
[70] Ansible facts website: https://docs.ansible.com/ansible/latest/user_guide/playbooks_vars_facts.html
[71] Prometheus website: https://prometheus.io/docs/prometheus/latest/getting_started
[72] ORY Ecosystem Project website: https://www.ory.sh/docs/ecosystem/projects/
[73] 3GPP (2020). 3GPP, TS 29.502, "5G System; Session Management Services;" version 15.6.0 Release 15, January 2020. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3340
[74] 3GPP (2016). 3GPP, TS 23.502, "Procedures for the 5G System (5GS)" Release 15, June 2016. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145
[75] Intel hyper threading technology website: https://www.intel.com/content/www/us/en/architecture-and-technology/hyper-threading/hyper-threading-technology.html
[76] ISO Standard website: https://www.iso.org/standard/66510.html
[77] O-RAN website: https://www.o-ran.org/
[78] A. Papageorgiou, et al. (2020). "On 5G network slice modelling: Service-, resource-, or deployment-driven?." in Computer Communications 149, 232-240, doi: 10.1016/j.comcom.2019.10.024
[79] Next Generation Mobile Network website: https://www.ngmn.org/
[80] OSM Scope and Functionality website: https://osm.etsi.org/wikipub/index.php/OSM_Scope_and_Functionality

[81] ETSI (2020). ETSI GS NFV 003, V1.5.1 (2020-01) "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV". Available at: https://www.etsi.org/deliver/etsi_gr/NFV/001_099/003/01.05.01_60/gr_NFV003v010501p.pdf

[82] ETSI (2020). ETSI GS NFV-TST 008 V3.3.1 (2020-06): "Network Functions Virtualisation (NFV) Release 3; Testing; NFVI Compute and Network Metrics Specification". Available at: https://www.etsi.org/deliver/etsi_gs/NFV-TST/001_099/008/03.03.01_60/gs_NFV-TST008v030301p.pdf

[83] ETSI (2020). ETSI GS NFV-IFA 013 V3.4.1. (2020-06): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification". Available at: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/013/03.04.01_60/gs_NFV-IFA013v030401p.pdf

[84] ETSI (2016). ETSI GS NFV-IFA 005 V2.1.1 (2016-04): "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification". Available at: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/005/02.01.01_60/gs_NFV-IFA005v020101p.pdf

[85] ETSI (2020). ETSI GS NFV-SOL 006 V3.3.1 (2020-08): "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; NFV descriptors based on YANG Specification". Available at: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/006/03.03.01_60/gs_NFV-SOL006v030301p.pdf

[86] ETSI (2016). ETSI GS NFV-IFA 014 V2.1. (2016-10): "Network Functions Virtualisation (NFV); Management and Orchestration; Network Service Templates Specification". Available at: https://www.etsi.org/deliver/etsi_gs/nfv-ifa/001_099/014/02.01.01_60/gs_nfv-ifa014v020101p.pdf

[87] ETSI (2016). ETSI GS NFV-IFA 011, "Network Functions Virtualisation (NFV); Management and Orchestration; VNF Packaging Specification". Available at: https://www.etsi.org/deliver/etsi_gs/nfv-ifa/001_099/011/02.01.01_60/gs_nfv-ifa011v020101p.pdf

[88] ETSI (2020). ETSI GS NFV-IFA 040 V4.1.1 (2020-11): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification". Available: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/040/04.01.01_60/gs_NFV-IFA040v040101p.pdf

[89] ETSI (2018). ETSI GS NFV-SEC 014 V3.1.1. (2018-04): "Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points". Available at: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/014/03.01.01_60/gs_nfv-sec014v030101p.pdf

[90] OSM White Paper "EXPERIENCE WITH NFV ARCHITECTURE, INTERFACES, AND INFORMATION MODELS" May 2018. Available at: https://osm.etsi.org/images/OSM_White_Paper_Experience_implementing_NFV_specs_final.pdf

[91] Nearby Computing NeabyOne website: https://www.nearbycomputing.com/project/nearbyorchestrator/

[92] Grafana website: https://grafana.com/

[93] Apache Kafka Website: https://kafka.apache.org/

[94] Gnocchi Website: https://gnocchi.xyz/

[95] CORSI, Antonello; ENG, Giampaolo Fiorentino. Deliverable 3.2 NRG-5 Application logic framework. 2017.

[96] Alvarez, F., Breitgand, D., Griffin, D., Andriani, P., Rizou, S., Zioulis, N., et al (2019). An edge-to-cloud virtualized multimedia service platform for 5G networks. IEEE Transactions on Broadcasting, 65(2), 369-380.

[97] OpenStack Horizon website: https://docs.openstack.org/horizon/latest/

[98] OpenStack Nova website: https://docs.openstack.org/nova/latest/
[99] OpenStack Neutron website: https://docs.openstack.org/neutron/pike/
[100] OpenStack Keystone website: https://docs.openstack.org/keystone/latest/
[101] OpenStack Heat website: https://docs.openstack.org/heat/latest/
[102] CloudStack website: https://cloudstack.apache.org/
[103] Sun, Y., Liu, Y., Tian, F., Wen, Q., & Jiang, L. (2021). Research on Traffic Dispatching Scheme of Multi-service Data Center for 5G Smart Grid. In Journal of Physics: Conference Series (Vol. 1746, No. 1, p. 012059). IOP Publishing
[104] OpenNebula website: https://opennebula.io/
[105] Libvirt website: https://libvirt.org/
[106] Open Nebula 5G Edge Cloud website: https://opennebula.io/building-5g-edge-clouds-for-containers-with-opennebula-and-aws-wavelength/
[107] Ligato website: https://ligato.io/
[108] Cloudwan website: https://github.com/cloudwan
[109] OPAL-RT website: https://www.opal-rt.com/simulator-platform-op5707/
[110] Itrinegy website: https://itrinegy.com/ne-one-enterprise-range/
[111] MODBUs Messaging on TCP/IP: https://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf
[112] C37.118-2005, "IEEE Standard for Synchrophasors for Power Systems," in IEEE Std C37.118-2005 (Revision of IEEE Std 1344-1995), vol., no., pp.1-65, 22 March 2006, doi: 10.1109/IEEESTD.2006.99376
[113] IEC 61850:2021 SER Series, " Communication networks and systems for power utility automation - ALL PARTS". Available at: https://webstore.iec.ch/publication/6028
[114] ETSI (2019). ETSI GS NFV-SOL 001 V2.6.1 (2019-05). "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on TOSCA specification". Available at: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/001/02.06.01_60/gs_nfv-sol001v020601p.pdf
[115] Raspberry website: https://www.raspberrypi.org/
[116] M. K. Penshanwar, M. Gavande and M. F. A. R. Satarkar, "Phasor Measurement unit technology and its applications - a review," 2015 International Conference on Energy Systems and Applications, 2015, pp. 318-323, doi: 10.1109/ICESA.2015.7503363.
[117] C37.244-2013, "IEEE Guide for Phasor Data Concentrator Requirements for Power System Protection, Control, and Monitoring," in IEEE Std C37.244-2013 , vol., no., pp.1-65, 10 May 2013, doi: 10.1109/IEEESTD.2013.6514039.
[118] Ha, K, and Satyanarayanan, M. (2015), "OpenStack++ for Cloudlet Deployment". School of Computer Science, Carnegie Mellon University, Pittsburgh, USA. Available Online: https://www.cs.cmu.edu/~satya/docdir/CMU-CS-15-123.pdf
[119] European Telecommunications Standards Institute (ETSI); ETSI TS 133 501 V16.30.0 (2020-08): 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.3.0 Release 16). Available at: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf
[120] The Third Generation Partnership Project (3GPP): 3GPP TS 33.501 V16.3.0 (2020-07): Security Architecture and Procedures 3GPP for 5G System (Release 16). Available at: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/
[121] The Third Generation Partnership Project (3GPP): 3GPP TS 33.401 V17.0.0 (2021-12): 3GPP System Architecture Evolution (SAE); Security architecture (Release 17). Available at: https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/
[122] ETSI (2018). ETSI White Paper No.24: "MEC Deployments in 4G and Evolution Towards 5G", February 2018. Available at:

https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf

[123] ETSI (2018). ETSI White Paper No.23: "Cloud RAN and MEC: A Perfect Pairing", February 2018. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp23_MEC_and_CRAN_ed1_FINAL.pdf

[124] ETSI (2018). ETSI White Paper No.28: "MEC in 5G Networks", June 2018. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

8 Annex A: MEC Framework

8.1 MEC Framework according to ETSI GS MEC 003

MEC enables the implementation of mobile edge applications as software-only entities that run on top of a virtualisation infrastructure, which is located in or close to the network edge. The MEC framework shows the general entities involved. These can be grouped into system level, host level and network level entities.

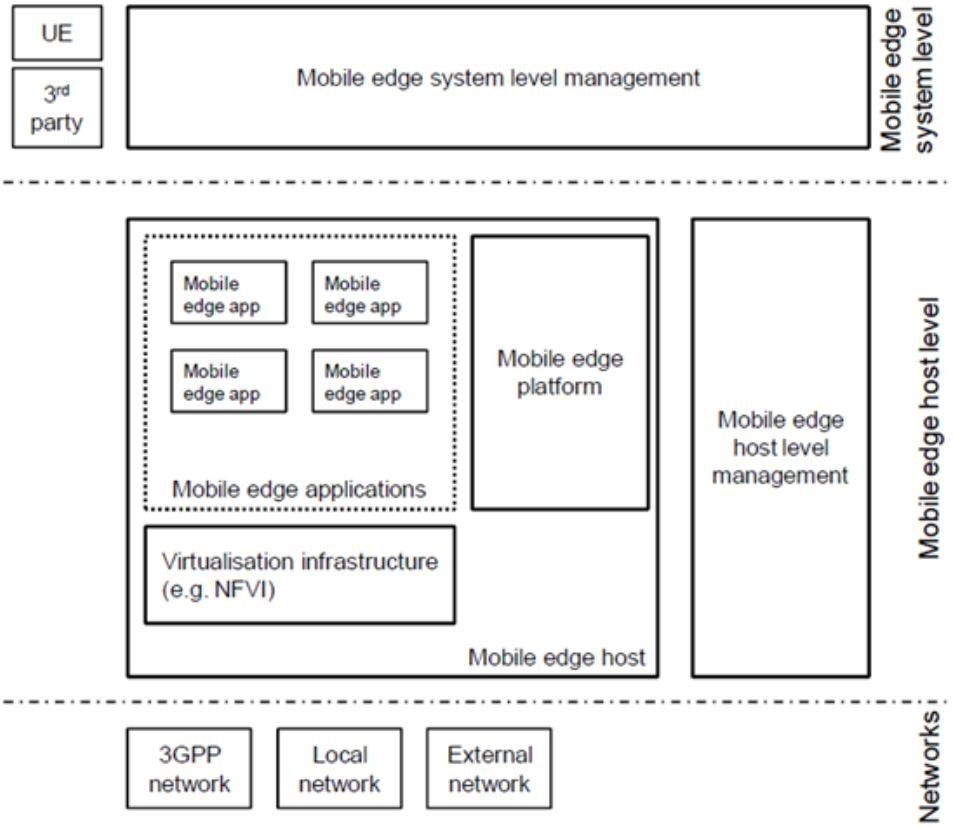

Figure 8-1 Multi-Access Edge Computing framework (according to ETSI GS MEC 003 [34])

Above, Figure 8-1 illustrates the framework for MEC consisting of the following distinct entities:

- Mobile edge host, including the following:
  - Mobile edge platform,
  - Mobile edge applications,
  - Virtualisation infrastructure;
- Mobile edge system level management;
- Mobile edge host level management;
- External related entities (i.e., network level entities).

The reference architecture shows the functional elements that comprise the mobile edge system and the reference points between them. The following figure depicts the mobile edge system reference architecture according to the ETSI GS MEC 003 approach [34]. There are three groups of reference points defined between the system entities, as follows:

- Reference points regarding the mobile edge platform functionality (Mp);

- Management reference points (Mm);
- Reference points connecting to external entities (Mx).

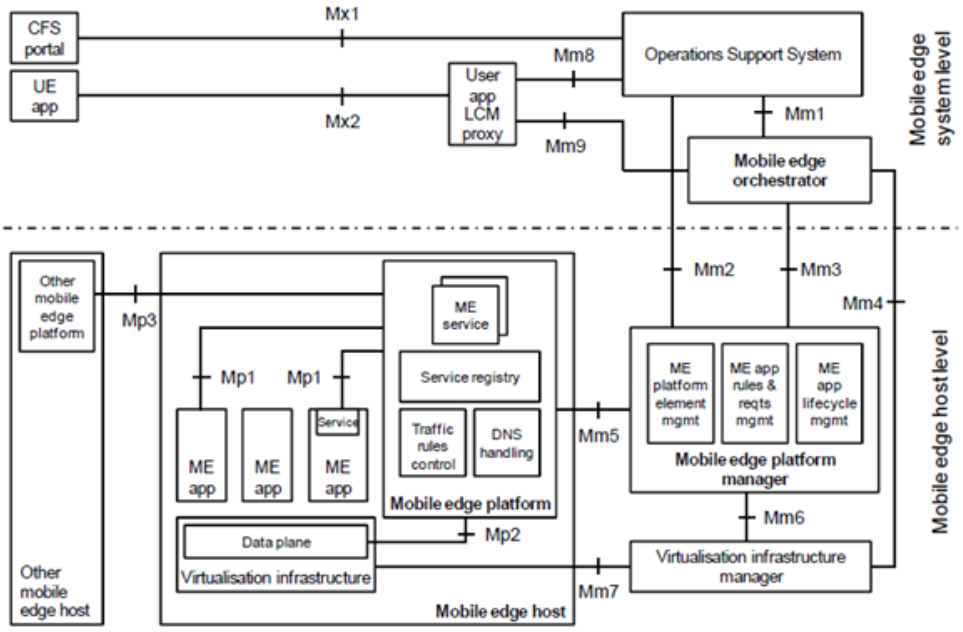

Figure 8-2 Mobile edge system reference architecture (according to ETSI GS MEC 003 [34])

The mobile edge system consists of the mobile edge hosts and the mobile edge management necessary to run mobile edge applications within an operator network – or a subset of an operator network.

The **mobile edge host** is an entity that contains a mobile edge platform and a virtualisation infrastructure which provides compute, storage, and network resources, for the purpose of running mobile edge applications. The virtualisation infrastructure includes a data plane that executes the traffic rules received by the mobile edge platform, and routes the traffic among applications, services, DNS (Domain Name System) server/proxy, 3GPP network, local networks, and external networks.

The **mobile edge platform** is the collection of essential functionalities required to run mobile edge applications on a particular virtualisation infrastructure and enables them to provide and consume mobile edge services. The mobile edge platform can also provide services and it is responsible for the following functions:

- Offering an environment where the mobile edge applications can discover, advertise, consume and offer mobile edge services, including, when supported, mobile edge services available via other platforms;
- Receiving traffic rules from the mobile edge platform manager, applications – or services – and instructing the data plane accordingly. When supported, this includes the translation of tokens representing UEs in the traffic rules into specific IP addresses;
- Receiving DNS records from the mobile edge platform manager and configuring a DNS proxy/server accordingly;
- Hosting mobile edge services;
- providing access to persistent storage and time of day information.

Mobile edge applications are instantiated on the virtualisation infrastructure of the mobile edge host based on configuration or requests validated by the mobile edge management. These are running as VMs on

top of the virtualisation infrastructure provided by the mobile edge host and can interact with the mobile edge platform to consume and provide mobile edge services. In certain cases, such applications can also interact with the mobile edge platform to perform certain support procedures related to the lifecycle of the application (such as indicating availability, preparing relocation of user state, etc.). Mobile edge applications can have a certain number of rules and requirements associated to them (such as required resources, maximum latency, required or useful services, etc.); these requirements are validated by the mobile edge system level management and can be assigned to default values, if missing.

The mobile edge management comprises the mobile edge system level management and the mobile edge host level management. The mobile edge system level management includes the mobile edge orchestrator as its core component, which has an overview of the complete mobile edge system.

The mobile edge orchestrator is responsible for the following functions:

- Maintaining an overall view of the mobile edge system based on deployed mobile edge hosts, available resources, available mobile edge services and topology.
- On-boarding of application packages, including checking the integrity and authenticity of the packages; validating application rules and requirements and, if necessary, adjusting them to comply with operator policies; keeping a record of on-boarded packages, and preparing the virtualisation infrastructure manager(s) to handle the applications.
- Selecting appropriate mobile edge host(s) for application instantiation based on constraints, such as latency, available resources and available services.
- Triggering application instantiation and termination.
- Triggering application relocation as needed when supported.

The Operations Support System (OSS) in Figure 8-2 refers to the OSS of an operator. It receives requests via the CFS (Customer Facing Service) portal and from UE applications for instantiation or termination of applications and decides on the granting of these requests. Granted requests are forwarded to the mobile edge orchestrator for further processing. When supported, the OSS also receives requests from UE applications for relocating applications between external clouds and the mobile edge system.

A user application is a mobile edge application that is instantiated in the mobile edge system in response to a request of a user via an application running in the UE (known as a UE application). The user application LCM proxy allows UE applications to request on-boarding, instantiation, termination of user applications and, when supported, relocation of user applications in and out of the mobile edge system. It also allows informing the UE applications about the state of the user applications.

The user application LCM proxy authorizes requests from UE applications in the UE and interacts with the OSS and the mobile edge orchestrator for further processing of such requests. The user application LCM proxy is only accessible from within the mobile network. It is only available when supported by the mobile edge system.

The CFS portal allows operators' third-party customers (e.g., commercial enterprises) to select and order a set of mobile edge applications that "meet" their particular needs, and to receive back service level information from the provisioned applications.

The mobile edge host level management comprises the mobile edge platform manager and the virtualisation infrastructure manager and handles the management of the mobile edge specific functionality of a particular mobile edge host and the applications running on it.

The mobile edge platform manager is responsible for the following functions:

- Managing the life cycle of applications including informing the mobile edge orchestrator of relevant application related events;
- Providing element management functions to the mobile edge platform;
- Managing the application rules and requirements including service authorizations, traffic rules, DNS configuration and resolving conflicts.

The mobile edge platform manager also receives fault reports and performance measurements from the virtualisation infrastructure manager for further processing.

The virtualisation infrastructure manager is responsible for the following functions:

- Allocating, managing and releasing virtualised (compute, storage and networking) resources of the virtualisation infrastructure;
- Preparing the virtualisation infrastructure to run a software image. The preparation includes configuring the infrastructure, and can include receiving and storing the software image;
- When supported, rapid provisioning of applications, as described in "OpenStack++ for Cloudlet Deployments";
- Collecting and reporting performance and fault information about the virtualised resources;
- When supported, performing application relocation. For application relocation from/to external cloud environments, the virtualisation infrastructure manager interacts with the external cloud manager to perform the application relocation.

Reference points related to the mobile edge platform are as follows:

Mp1: The Mp1 reference point between the mobile edge platform and the mobile edge applications provides service registration, service discovery and communication support for services. It also provides other functionality such as application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and time of day information, etc. This reference point can be used for consuming and providing service specific functionality.

Mp2: The Mp2 reference point between the mobile edge platform and the data plane of the virtualisation infrastructure is used to instruct the data plane on how to route traffic among applications, networks, services, etc. This reference point is not further specified.

Mp3: The Mp3 reference point between mobile edge platforms is used for control communication between mobile edge platforms.

Reference points related to the mobile edge management are as follows:

Mm1: The Mm1 reference point between the mobile edge orchestrator and the OSS is used for triggering the instantiation and the termination of mobile edge applications in the mobile edge system.

Mm2: The Mm2 reference point between the OSS and the mobile edge platform manager is used for the mobile edge platform configuration, fault and performance management.

Mm3: The Mm3 reference point between the mobile edge orchestrator and the mobile edge platform manager is used for the management of the application lifecycle, application rules and requirements and keeping track of available mobile edge services.

Mm4: The Mm4 reference point between the mobile edge orchestrator and the virtualisation infrastructure manager is used to manage virtualised resources of the mobile edge host, including keeping track of available resource capacity, and to manage application images.

Mm5: The Mm5 reference point between the mobile edge platform manager and the mobile edge platform is used to perform platform configuration, configuration of the application rules and requirements, application lifecycle support procedures, management of application relocation, etc.

Mm6: The Mm6 reference point between the mobile edge platform manager and the virtualisation infrastructure manager is used to manage virtualised resources (e.g. to realize the application LCM).

Mm7: The Mm7 reference point between the virtualisation infrastructure manager and the virtualisation infrastructure is used to manage the virtualisation infrastructure.

Mm8: The Mm8 reference point between the user application LCM proxy and the OSS is used to handle UE applications requests for running applications in the mobile edge system.

Mm9: The Mm9 reference point between the user application LCM proxy and the mobile edge orchestrator of the mobile edge system is used to manage mobile edge applications requested by UE application.

Reference points related to external entities are as follows:

Mx1: The Mx1 reference point between the OSS and the customer facing service portal is used by the third-parties to request the mobile edge system to run applications in the mobile edge system.

Mx2: The Mx2 reference point between the user application LCM proxy and the UE application is used by a UE application to request the mobile edge system to run an application in the mobile edge system, or to move an application in or out of the mobile edge system. This reference point is only accessible within the mobile network. It is only available when supported by the mobile edge system.

8.2 Deploying MEC in the 5G system architecture

The 5G SBA specified by 3GPP TS 23.501 [33] contains multiple control plane functional entities, like the Policy Control Function (PCF), the Session Management Function (SMF), the AF, data plane functional entities like the UPF, etc.

In contrast to the current 4G/4G+mobile network architecture, the 5G system was conceived to allow a more flexible deployment of the data plane, aiming to natively support edge computing. As a consequence, the MEC architecture can easily be integrated into that defined for 5G.

Figure 8-3 illustrates an example MEC mapping to the 5G system architecture, where for example the MEC host's data plane can be mapped to 5G's UPF element.

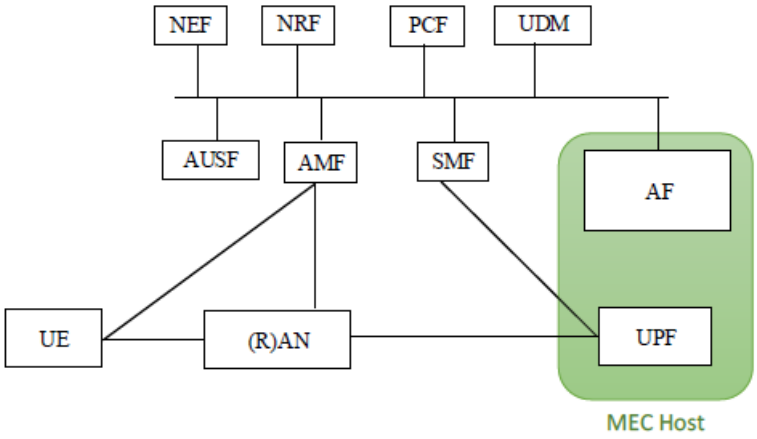

Figure 8-3 An example of MEC mapping with 5G system architecture (according to [122])

In the example above [122], the MEC platform would leverage the 5G network architecture and performs the traffic routing and steering function in the UPF. For example, a UL (Uplink) Classifier of UPF is used to divert to the local data plane the user traffic matching traffic filters controlled by the SMF, and further steer to the application. The PCF and the SMF can set the policy to influence such traffic routing in the UPF. Also, the AF via the PCF can influence the traffic routing and steering. Therefore, MEC in 5G is able to influence the UPF through the standardised control plane interface in SMF, similarly to some of the EPC (Evolved Packet Core) MEC deployment scenarios already examined in 4G.

Although the position of MEC at the edge site is left to the operators' choice, similarly to what has been done for the 4G MEC deployment, there are several migration examples to 5G selected architectures. The pictures below show how the MEC host, which includes the 4G CN functions, can be transformed to support 5G by software upgrading the relevant network functions. In the transition to 5G the MEC functionalities introduced with the 4G technology are preserved, fulfilling key requirements such as:

- Reusing the edge computing resources.
- Interaction with 5G control plane.
- Integration with the 5G network.

Figure 8-4 depicts several migration patterns from 4G towards 5G. We can briefly distinguish the following:

- In the top left diagram, MME (Mobility Management Entity), SGW (Serving Gateway), PGW (PDN (Packet Data Network) Gateway) and HSS (Home Subscriber Server) migration is depicted, e.g., to support private networks and mission critical applications.
- At the top right, it is depicted SGW-LBO (Serving Gateway with Local Breakout) MEC migration to 5G for selective traffic offloading.
- In the bottom diagram, it is depicted a CUPS (Control/User Plane Separation) migration to 5G.

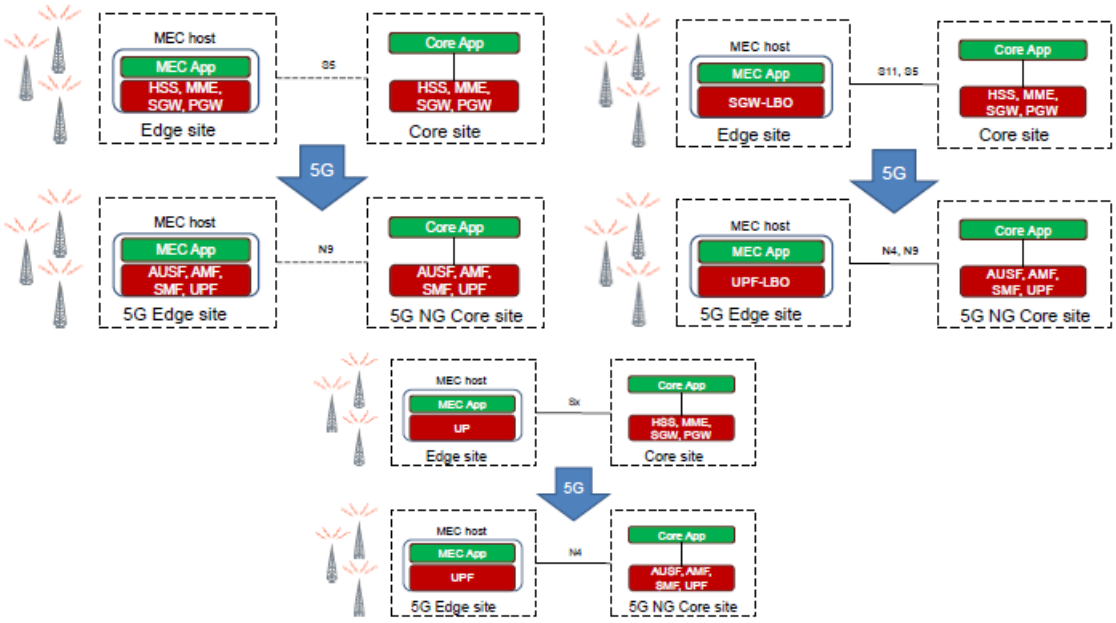

Figure 8-4 Migration patterns for MEC deployments from 4G to 5G (according to [122])

The 5G system architecture specified by 3GPP and described in 3GPP TS 23.501 [33] has been designed to cater for a wide set of UCs ranging from a massive amount of simple IoT devices to the other extreme of high bit rate, high reliability mission critical services. Supporting all the UCs with the same and common architecture has required significant changes in design philosophies both for the RAN and the CN. In particular, CRAN and MEC are highly complementary technologies. Collocating these helps make the economics of each of them significantly more attractive. Collocating CRAN and MEC also helps an MNO to support (and generate revenue from) some of the key 5G applications that it would not be able to support otherwise [123].

One significant architectural change was made to the communications between the CN functions that have previously relied on a point-to-point paradigm. In the 5G system specification there are two options available for the architecture: one with the traditional reference point and interface approach and the other where the CN functions interact with each other using a SBA. With the SBA, there are functions that consume services and those that produce services. Any network function can offer one – or more – services. The framework in [34] provides the necessary functionality to authenticate the consumer and to authorise its service requests. This framework also supports flexible procedures to efficiently expose and consume services. For simple service or information requests, a request-response model can be used. For any long-lived processes, the above framework also supports a subscribe-notify model. The API framework defined by ETSI ISG MEC is aligned with these principles and does exactly the same for MEC applications, as the SBA does for network functions and their services. The functionality needed for efficient use of the services includes registration, service discovery, availability notifications, de-registration, and authentication and authorisation. All this functionality is the same in both the SBA and the MEC API frameworks.

In the figure below the 3GPP 5G system with its SBA is shown on the left, while the MEC system architecture is depicted on the right. In the continuity of the document the focus is upon describing how to deploy the MEC system in a 5G network environment in an integrated manner, where some of the functional entities of MEC (blue boxes in MEC system part) interact with the network functions of the 5G CN.

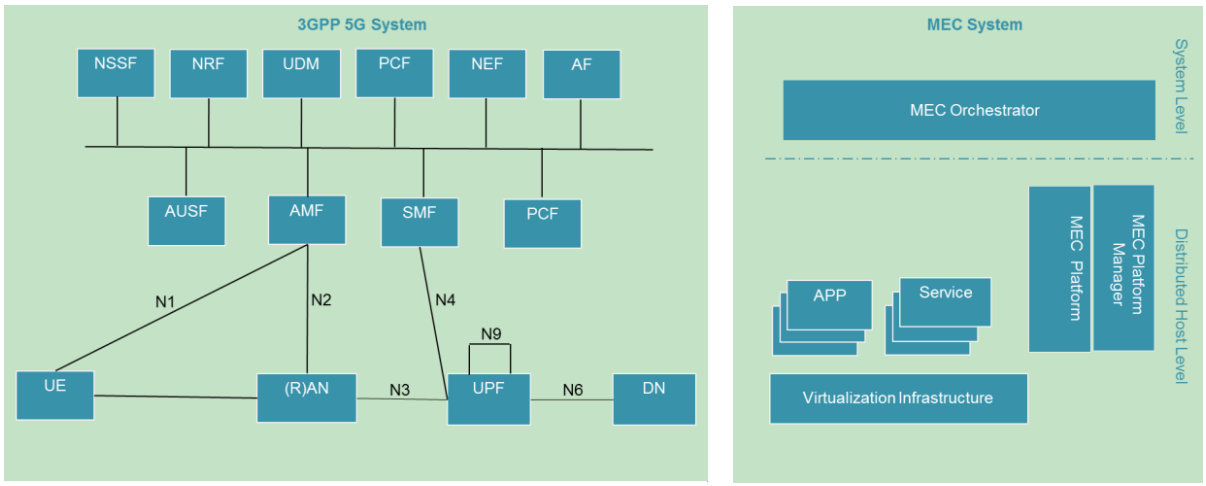

Figure 8-5 5G Service-Based Architecture and a generic MEC architecture (according to [124]).

The network functions and the services they produce are registered in a Network Resource Function (NRF) while in MEC the services produced by the MEC applications are registered in the service registry of the MEC platform. Service registration is part of the Application Enablement functionality [27]. To use the service, if authorised, a network function can directly interact with the network function that produces the service. The list of available services can be discovered from the NRF. Some of the services are accessible only via the NEF, which is also available to untrusted entities that are external to the domain. In other words, the NEF acts as a centralised point for service exposure and also has a key role in authorising all access requests originating from outside of the system.

In addition to AF, NEF and NRF, there are a number of other functions that are worth introducing. The procedures related to authentication are served by the Authentication Server Function (AUSF).

One of the key concepts in 5G is Network Slicing that allows the allocation of the required features and resources from the available network functions to different services or to tenants that are using the services. The Network Slice Selection Function (NSSF) is the function that assists in the selection of suitable NSIs for users and in the allocation of the necessary Access Management Functions (AMF). A MEC application, that is an application hosted in the distributed cloud of a MEC system can belong to one or more network slices that have been configured in the 5G CN.

Policies and rules in the 5G system are handled by the PCF. The PCF is also the function whose services an AF, such as a MEC platform, requests in order to impact the traffic steering rules. The PCF can be accessed either directly, or via the NEF, depending whether the AF is considered trusted – or not – and in the case of traffic steering, whether the corresponding PDU (Protocol Data Unit) session is known at the time of the request.

The Unified Data Management (UDM) function is responsible for many services related to users and subscriptions. It generates the 3GPP AKA (Authentication and Key Agreement) authentication credentials; handles user identification related information; manages access authorization (e.g., roaming restrictions); registers the user serving NFs (serving AMF, SMF); supports service continuity by keeping record of SMF/Data Network Name (DNN) assignments; supports Lawful Interception (LI) procedures in outbound roaming by acting as a contact point, and performs subscription management procedures.

The UPF has a key role in an integrated MEC deployment in a 5G network. UPFs can be seen as a distributed and configurable data plane from the MEC system perspective. The control of that data plane (i.e., the traffic rules configuration) follows the NEF-PCF-SMF route. Consequently, in some specific deployments the local UPF may even be part of the MEC implementation.

Figure 8-6 shows how the MEC system is deployed in an integrated manner in 5G network.

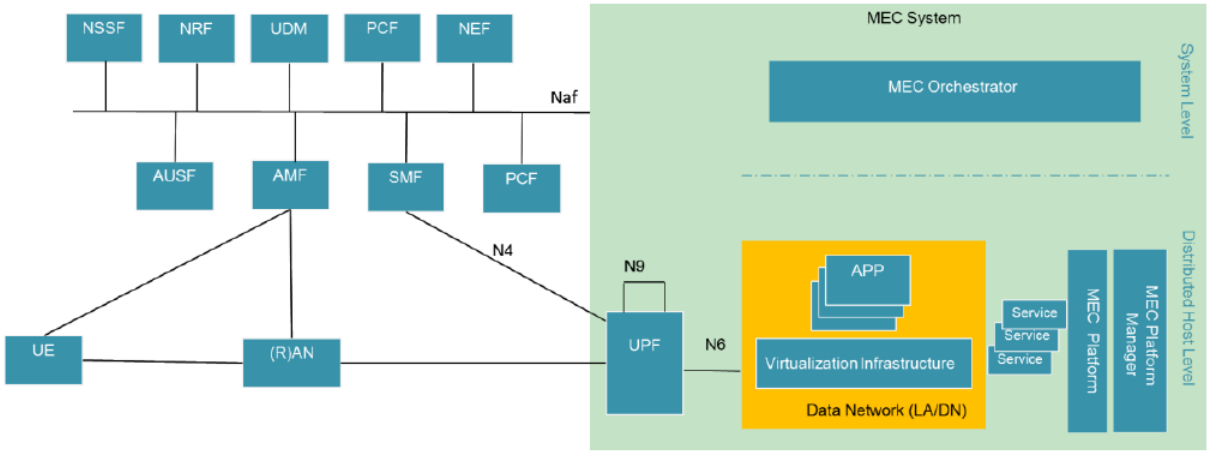

Figure 8-6 5G Service Integrated MEC deployment in the 5G network (according to [124]).

In the MEC system on the right-hand side of Figure 8-6, the MECO is a MEC system level functional entity that, acting as an AF, can interact with the NEF, or in some scenarios directly with the target 5G NFs. On the MEC host level it is the MEC platform that can interact with these 5G NFs, again in the role of an AF. The MEC host (i.e.: the host level functional entities) are most often deployed in a data network in the 5G system. While the NEF as a CN function is a system level entity deployed centrally together with similar NFs, an instance of NEF can also be deployed in the edge to allow low latency, high throughput service access from a MEC host.

MEC can be deployed on the N6 reference point that is in a data network external to the 5G system. This is enabled by flexibility in locating the UPF. The distributed MEC host can accommodate, apart from MEC apps, a message broker as a MEC platform service and another MEC platform service to steer traffic to local accelerators. The choice to run a service as a MEC app or as a platform service is likely to be an implementation choice and should factor in the level of sharing and authentication needed to access the service. A MEC service such as a message broker could be initially deployed as a MEC app to gain time-to-market advantage, and then become available as a MEC platform service as the technology and the business model matures.

Managing user mobility is a central function in a mobile communications system. In a 5G system it is the AMF that handles mobility related procedures. In addition, the AMF is responsible for the termination of RAN control plane and Non-Access Stratum (NAS) procedures, protecting the integrity of signalling, management of registrations, connections and reachability, interfacing with the lawful interception function for access and mobility events, providing authentication and authorisation for the access layer, and hosting the Security Anchor Functionality (SEAF). With the SBA, the AMF provides communication and reachability services for other NFs. Besides, it allows subscriptors to receive notifications regarding mobility events.

Similarly to the AMF, the SMF is in a key position with its large number of responsibilities. Some of the functionality provided by the SMF includes session management, IP address allocation and management, DHCP (Dynamic Host Configuration Protocol) services, selection/re-selection and control of the UPF, configuring the traffic rules for the UPF, lawful interception for session management events, charging, and support for roaming. As MEC services may be offered in both centralised and edge clouds, the SMF plays a critical role due to its role in selecting and controlling the UPF and configuring its rules for traffic steering. The SMF exposes service operations to allow MEC as a 5G AF to manage the PDU sessions, control the policy settings and traffic rules as well as to subscribe to notifications on session management events.